DESIGNED TO WIN:

AN AGILE APPROACH TO AIR FORCE COMMAND AND CONTROL OF CYBERSPACE

BY

JOHN P. SMAIL

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2010

APPROVAL

The undersigned certify that this thesis meets masters-level standards of research, argumentation, and expression.

_____

COL MICHAEL W. KOMETER (Date)

_____

DR. JOHN B. SHELDON (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Lieutenant Colonel John P. Smail is a cyberspace operations officer with experience in both fixed and deployable communications. He enlisted in the Air Force in 1986 and received his commission in 1996 through the Air Force Officer Training School. He has deployed in support of Operation DESERT SHIELD, DESERT STORM, ALLIED FORCE, NORTHERN WATCH, IRAQI FREEDOM, and the humanitarian response to Hurricane Katrina. He is a graduate of Georgia College and State University, earning a B.B.A. in Information Systems Management and Bowie State University, earning a M.S. in Management Information Systems. Before SAASS, Lieutenant Colonel Smail graduated from the US Army Command and Staff College, Fort Leavenworth, KS. Lieutenant Colonel Smail has been selected as the commander, 455th Expeditionary Communications Squadron, Bagram Air Base, Afghanistan in support of Operation ENDURING FREEDOM.

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to my research advisor, Colonel Michael Kometer, for his guidance, support, and giving me incredible freedom to explore cyberspace and perform the research that I felt was important. I thank my reader, Dr. John B. Sheldon, for lending his expertise, interest, and support of this excursion into cyberpower. Special thanks to Lieutenant Colonel Jeff Boleng for his thoughts and critiques as I developed the ideas put forth in this paper.

Finally, and most importantly, I would like to express my most heartfelt appreciation to my wife. Her love and understanding during the year has provided the greatest support and kept me motivated to complete the rigorous academic course work.

ABSTRACT

This study analyzes the need for the Air Force to design a cyberspace command and control approach that can survive and respond to the demands of a high-level conflict against a near-peer opponent. The conclusion is that the cyberspace domain is subject to the same challenges of the other war-fighting domains and command and control approaches that attempt to achieve perfect situational awareness and centralized control will fail; putting operations in all war-fighting domains at risk. The author provides a history of command and control in the land, sea, and air domains and discusses how technology influenced the decision to centralize or decentralize command and control. Next, the writer describes the current Air Force command and control approach for air, space, and cyberspace and demonstrates through a scenario how the different elements interact to control a time sensitive target event that traverses all three Air Force domains. Using this information, the author compares and contrasts the domains and provides recommendation on the most agile command and control approach for Air Force cyberspace. Finally, this paper proposes how the Air Force may best posture its forces to command and control the domain to win a high-level conflict against a near-peer competitor.

CONTENTS

Illustrations

Figure

Introduction

> *Cyberspace pervades every other domain and transcends traditional boundaries. Without question, cyberspace is vital to today's fight and to the future US military advantage over our adversaries.*
>
> — *Honorable Michael B. Donley and General Norton A. Schwartz*

The Air Force should take a more agile approach to command and control of cyberspace to maintain network access and continue operations during significant and persistent cyber attacks. The current command and control structure for Air Force cyber forces is designed to defend, operate, and maintain the Air Force network. However, millions of network intrusions continue unabated while services and information access are further restricted in an effort to protect the network. To combat this threat, the Air Force and Department of Defense (DOD) have begun to develop doctrine and restructure forces to ensure access to the domain, but it is unclear what the operational philosophy is with respect to maintaining access, conducting attacks, and ensuring support to air, land, and space operations. The Air Force must design a cyberspace command and control approach to survive and respond to the demands of a high-level conflict against a near-peer opponent or the operations in all war-fighting domains will be at risk.

This paper will attempt to determine the most effective approach to the command and control of Air Force cyber forces. Historically, the approach to command and control has been significantly influenced by the technology available and the commander's ability to utilize it to control his forces. Experience shows that military force is optimized when commanders match the capabilities and limitations of technology with a level of control that synchronizes operations, yet allows independent action to take advantage of fleeting opportunities. The Air Force has accumulated ample historical experience to suggest the most appropriate doctrine for the command and control of air and space. Although continually attacked during low-level conflicts, cyberspace has yet to be challenged by a near-peer competitor during a high-level conflict. Will the command and control approach applied today function or fail when cyberspace is needed most? To be successful, the organization, training, and equipping of Air Force cyberspace forces must

take advantage of the unique attributes of the cyberspace domain and be agile enough to meet the demands of a high paced conflict.

As an introduction to the domain, a definition of cyberpower is presented to clarify and encapsulate the elements that make cyberspace a war-fighting domain. Then cyberpower's relation to air and space power is explored to describe how, although cyberpower is different, its primarily purpose is to enable operations in all the war-fighting domains. To introduce the cyberspace challenge, this paper presents a background of the threats to both public and private cyberspace through a short description of how the cyber attacks on Georgia during the 2008 Russian invasion of South Ossetia is most probably a preview of the future of military conflicts. Finally, the Joint and Air Force definitions of command and control are presented.

This analysis will look at the command and control of cyberspace from the operational level of warfare, below the grand strategic and military strategic level so as not to delve into the many intractable issues of civil-military relations in regards to attack and defense of the much larger and diverse civilian portion of cyberspace. Understanding that conflict in cyberspace is, and will be, conducted against all elements of power, this analysis is concerned with the command and control of the Air Force portion of the Global Information Grid, or those portions thereof that the Air Force is responsible to defend, operate, and maintain.

Background

From the first time humans harnessed the power of the musket and cannon, through the industrial revolution, the nuclear era, and into to the information age, the advance of technology has continuously influenced the West. Western militaries, in particular, have used technology in war and attempted to develop the superior weapon and provide the commander with perfect information to guarantee victory.[1] New technologies developed during World War II inspired the father of cybernetics, Norbert Wiener, "to view the world as information, which he understood in terms of communications and control."[2] Although today's technology is dramatically more

[1] Although technology is developed and utilized in warfare by almost all cultures, western militaries have been especially adept at responding to and adopting technology. Geoffrey Parker, ed., *The Cambridge History of Warfare* (New York, NY: Cambridge University Press, 2005), 2.

[2] Adam Brate, *Technomanifestos* (New York, NY: TEXERE LLC, 2002), 12.

scalable and capable, Wiener's view of information has proven remarkably prescient. The use of information technology has proliferated on and off the battlefield and its use has become integral to every military competency, all of which operate in the war-fighting domain of cyberspace.

The United States economy, government, defense, and society are extremely reliant on uninterrupted access to cyberspace. Today that domain is under constant attack. Enemies of the United States understand the asymmetric advantage cyberspace provides the military, especially the Air Force, and the disruption of this access can have significant impacts to mission effectiveness. The Internet and military networks employed today are based on protocols that were developed with open standards, fault tolerance, and sharing as the primary purpose.[3] This open architecture can be at odds with the requirement for security, privacy, and attribution.

Until the 1990's, most computers used for command and control were mainframe systems with very limited access.[4] Security concerns were minimal and measures consisted primarily of physical security of the terminals and password controls. Since that time, the Air Force has in effect connected its command and control system to both friends and competitors via the Internet. The Internet, being an open system, is replete with hackers, hacktivists, criminals, and military cyber adversaries that can cause damage to Air Force systems. Trojan horses, worms, viruses and other forms of malware can spread from systems thought to be friendly at the speed of light. Most of the damage experienced is temporary, but the effects can be devastating if loss of communication occurs during a critical operation. Hackers can execute denial of service attacks from millions of computers across the world to target a specific system. Response is difficult to impossible because definitively attributing an attack to a specific actor is very difficult.[5] Computer and network hardware security can be even more challenging than

---

[3] The Internet Society, RFC: 3365 "Strong Security Requirements for Internet Engineering Task Force Standard Protocols," August 2002. http://www.rfc-editor.org/rfc/rfc3365.txt (accessed 26 May 2010).
[4] The Worldwide Military Command and Control System (WMMCCS) was the DOD's centralized, command and control system during the Cold War. It consisted primarily of mainframe computers, terminals, and data networks. During the 1990s, the DOD transitioned to less centralized systems incorporating commercial-off-the-shelf technology. See David E. Pearson, *The World wide Military Command and Control System: Evolution and Effectiveness* (Maxwell AFB, AL: Air University Press, 2000), 331-340.
[5] Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York, NY: Oxford University Press, 2009), 6-10.

securing software. Microprocessors, composed of millions of integrated circuits, make up the end devices and the equipment that move the traffic on the Internet. The equipment the DOD employs to communicate and to control weapon systems is manufactured throughout the world. Recent events have led some to believe that states have manufactured purposeful faults into some chips to cause them to respond to outside commands to shut down. For example, IEEE speculated that during the 2007 Israel attack on a Syrian nuclear reactor "the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden "backdoor" inside" and sent a command to temporarily disable the radar's ability to track Israeli jets.[6] In response, DARPA has begun its Trust in Integrated Circuits program to certify that the integrated circuits going into US weapon systems do not contain malicious circuits.[7] However, this problem is a tremendous challenge considering the complexity of the microprocessors and the number of chips the military uses throughout the force. Although a necessary effort, there is no guarantee of success.

Enemies of the United States will contest access to cyberspace during both limited and conventional conflicts. As many developing nations modernize their defense systems, they are increasingly reliant on cyberspace and exposed to cyber threats. For example, in 2008 a dispute between Georgian and Russian-led peacekeeping forces resulted in Russian forces invading the Republic of Georgia's semi-autonomous region of South Ossetia. For several days before the invasion, Georgian governmental and civilian websites became the target of increasing cyber attacks. On 8 August 2008, as the ground attack commenced, several Georgian state computer servers came under external control. Targeting the Georgian President, Ministry of Foreign Affairs, Ministry of Defence, the central government, and Georgian commercial websites, the ability of the Georgian government to communicate with its citizens during the most critical point in the conflict was seriously impaired.[8]

Due to the significance of cyberspace to the United States, it is imperative that the nation dedicate the required resources, labor, and innovative talent necessary to ensure

---

[6] Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum.* May 2008. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch (accessed 5 February 2010).
[7] Adee, "Hunt for the Kill Switch".
[8] Eneken Tikk et al, *Cyber Attacks Against Georgia: Legal Lessons Identified.* Analysis, Tallin, Estonia: Cyber Cooperative Centre of Excellence, 2008.

access to cyberspace in order to achieve national objectives.[9] This will require cyberspace be treated as a separate domain from air and space to create a professional force specialized in the environment and able to articulate its proper application at the strategic, operational, and tactical levels of war.

The Cyberspace Domain

Science fiction novelist William Gibson first used the word cyberspace to describe a matrix simulator in his short story "Burning Chrome", a story about two hackers who use Russian hacking software to attack an organized crime ring's computer systems.[10] Subsequently, in his novel *Nueromancer*, Gibson uses the term to describe "a custom cyberspace deck that projected his disembodied consciousness into the consensual hallucination that was the matrix."[11] The term has since become synonymous for anything dealing with computers and the Internet, and eventually fully adopted by the DOD to describe an operational war-fighting domain of operations equal to the air, land, sea, and space.

As a new operational area evolves, it can challenge the beliefs, attitudes, and occupational specialties service members hold dear. The definitions of cyberpower and cyberspace can be quite contentious and subject to a wide range of understandings and interpretations. The official definition of cyberspace, promulgated through the National Security Presidential Directive-54 / Homeland Security Presidential Directive-23 (Cybersecurity Policy) dated 8 January 2008 and repeated in Joint Publication 1-02 states cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." This definition is deficient in that it does not provide a clear distinction between the other physical domains by acknowledging the fact that the transport mechanism for cyberspace is the electromagnetic spectrum.[12]

---

[9] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), 272.
[10] William Gibson, "Burning Chrome," in *Burning Chrome* (New York, NY: HarperCollins Publishers Inc., 1986), 179.
[11] William Gibson, *Neuromancer* (New York, NY: Penguin Group, 1984), 5.
[12] Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer et al. (Washington, DC: National Defense University Press, 2009), 31.

A more comprehensive definition of cyberspace is necessary to clarify how cyberspace is different from the domains of air, land, sea, and space and to describe how human innovation is responsible for the domain's existence. Dan Kuehl's identifies fourteen different proposed definitions of cyberspace before adding his own.[13] Kuehl's definition most closely captures cyberspace as discussed in this paper, where "cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies."[14] This definition is sufficiently broad enough to include both the manufactured technologies and the environmental aspects normally associated with cyberspace, yet bounds the domain to one that is identifiable and is the working definition used in this paper.

Cyberspace encompasses a tremendous network that spans the public and private domains. The Air Force has sole responsibility to protect and operate its portion of the DOD's Global Information Grid (GIG). DOD Directive (DoDD) 8000.01, *Management of the Department of Defense Information Enterprise,* defines the GIG as "The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network."[15] The Air Force Information Network (AFIN) is the portion of the GIG that includes all the core networks and services, administrative, and mission systems supporting Air Force operations. The ubiquitous nature of cyberspace means that although the Air Force has sole responsibility for portions of the GIG, it must interact with other military services, government agencies, and private organizations together to ensure freedom of action.

---

[13] Kuehl, "Cyberspace to Cyberpower," 26.
[14] Kuehl, "Cyberspace to Cyberpower," 28.
[15] DOD Directive (DODD) 8000.1, *Management of the Department of Defense Information Enterprise*, 10 February 2009.

Cyberspace is largely a manufactured domain. The computer hardware and software, network equipment, and infrastructure define its character and reveal its strengths and weaknesses. The argument that cyberspace differs from the other operational domains of air, land, sea, and space because it is a domain created by humans belies that fact that all the war-fighting domains utilize man-made machinery to use the domains.[16] Cyberspace is unique in that the technology is constantly changing; the medium involves the movement of information; and in the respect that it permeates through and in all the other physical domains at nearly the speed of light. It is unimaginable for the current sailor, soldier, marine, or airman to operate without cyberspace. Cyberspace has become a war-fighting domain by simultaneously gaining critical importance in the civilian and the military communities, and the technology and its benefits are easily transferred from one community to the other.

The Nature of Cyberpower

When the military services discuss their core competencies, they typically do so in reference to the domain in which they fight. The Air Force has traditionally discussed the proper employment of air and space power; and has now added cyber power.[17] Dan Kuehl proposes that the definition of cyberpower is "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[18] This definition is not a comparison of service capabilities, but reflects the omnipresent nature of cyberpower throughout the military, government, and civilian communities. For example, President Obama's *Cyberspace Policy Review* addressed the government's responsibility of defending cyberspace as key to the security of the nation, "the Federal government cannot entirely delegate or abrogate its role in securing the Nation from a cyber incident or accident."[19] Although the infrastructure of cyberspace is prominently a private enterprise, its importance to the well-being of the nation cannot be ignored. A coordinated effort between the government and private sector is imperative to ensuring access to cyberspace and wielding cyberpower.

---

[16] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 5.
[17] Department of the Air Force, *Fiscal Year 2010 Air Force Posture Statement*, 19 May 2009, 3.
[18] Kuehl, "Cyberspace to Cyberpower," 24-42.
[19] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications infrastructure* (Washington, DC: The White House, 2009), iv.

JP 1-02 defines cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid." The Air Force and DOD must integrate cyberspace operations with operations in the other domains. For example, offensive cyberspace operations such as a network attack on a power station or communications node can create important effects in the other war-fighting domains. Although all airmen can conduct cyberspace operations, this paper will use the term "cyberspace operator" to refer to the communications specialists that are responsible for the operations, maintenance, defense, attack, and exploitation missions unless otherwise stated.[20]

The draft Air Force Doctrine Document for Cyberspace Operations defines cyberspace superiority as "that degree of dominance in cyberspace of one force over another that permits the conduct of operations by the former and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by the opposing force."[21] The *National Military Strategy for Cyberspace Operations* is the US Armed Forces comprehensive strategy to ensure superiority in cyberspace. The strategy directs four strategic priorities that provide focus for a wide range of outcomes:[22]

- Gain and maintain initiative to operate within adversary decision cycles
- Integrate cyberspace capabilities across the range of military operations
- Build capacity for cyberspace operations
- Manage risk for operations in cyberspace

The Air Force added cyberspace superiority as one of its twelve core functions in its *Fiscal Year 2010 Air Force Posture Statement*.[23] The addition of the cyberspace domain to the Air Force mission requires that the service make a serious investment in the organization, training, and equipping of a force structure to use cyberpower. Therefore, it is imperative that the Air Force wield cyberpower adroitly to enable

[20] The current Twenty-fourth Air Force commander, Maj Gen Webber stated he considers all airmen cyberspace operators because they are critical to the defense of the network through responsible actions and activities. Interview by author, 22 March 2010.
[21] Air Force Doctrine Document (AFDD) 3-12 (Draft), *Cyberspace Operations*, XX March 2010, 3.
[22] Secretary of Defense, *The National Military Strategy for Cyberspace Operations* (Washington DC: Department of Defense, December 2006), 19. Document is now declassified.
[23] Department of the Air Force, Presentation to the Senate Armed Services Committee, United States Senate, *Fiscal Year 2010 Air Force Posture Statement*, 21 May 2009, 1.

operations in the other war-fighting domains. This will include the development of cyber forces, doctrine, and a command and control structure to execute operations.

What is Command and Control?

Command and control, although a modern term to be sure, is anything but new to the art of warfare. As Martin van Creveld writes in his historical investigation of Command, Control, and Communications, or as he abbreviates, 'command', "the problem of commanding and controlling armed forces, and of instituting effective communications with and within them, is as old as war itself."[24]

At its most basic form, command and control is about focusing the efforts of an organization's resources, information, and assets towards the attainment of an objective.[25] The Air Force recognizes the importance of command and control to mission accomplishment by designating it one of the key operational functions of air and space power.[26] Joint Publication 1-02 and Air Force Doctrine Document (AFDD) 2-8 define Command and Control as "the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and Control is performed through an arrangement of personnel, equipment, communications, facilities and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission."[27] With this definition, the following are functions of command and control for a specific undertaking:[28]

- Establishing intent (the goal or objective)
- Determining roles, responsibilities, and relationships
- Establishing rules and constraints (schedules, etc.)
- Monitoring and assessing the situation and progress
- Inspiring, motivating, and engendering trust
- Training and education

---

[24] Martin Van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), 1.
[25] David S. Alberts and Richard E. Hayes, *Understanding Command and Control* (Washington D.C.: DoD Command and Control Research Program, 2006), 32, 67.
[26] Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, 17 November 2003, 49.
[27] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (amended 31 October 2009), 101.
[28] Alberts and Hayes, *Understanding Command and Control*, 34.

The Air Force command and control construct places the commander in the center of the Air Force command and control construct with C2 Systems and Technology as a key enabler to effective decision-making by the commander. Figure 1, from AFDD 2-8, portrays "command and control as the lens through which Air Force forces are transformed into air and space power, and it enables accomplishment of the mission."[29]

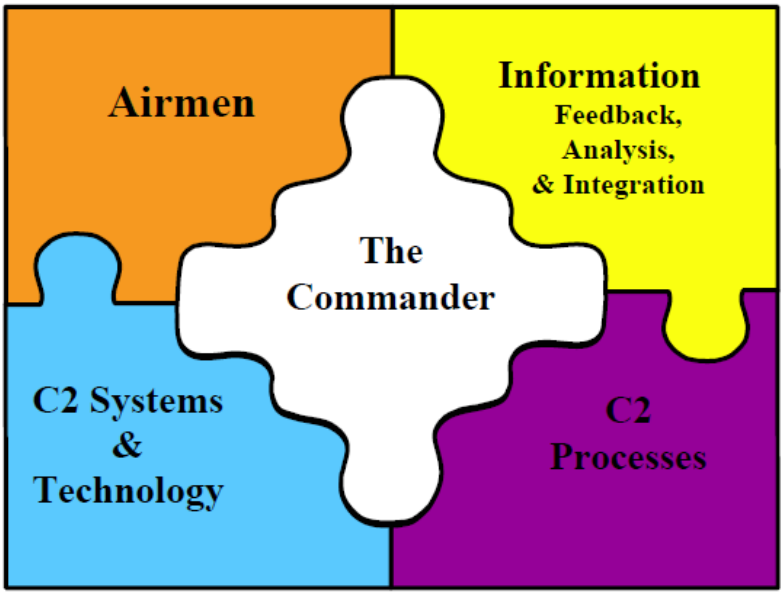

Figure 1: The Air Force C2 Construct
Source: Air Force Doctrine Document 2-8, Command and Control, 1 June 2007

The Air Force doctrine for command and control is grounded on the key tenet of air and space power centralized control and decentralized execution.[30] Due to their limited numbers and strategic importance across multiple geographic areas, Air Force space forces are typically commanded and controlled with centralized control and centralized execution.[31] Cyberspace has unique characteristics that demand a command and control approach different from air and space. The offensive form of warfare is dominant in cyberspace and allows both state and non-states actors to operate with stealth and anonymity to take advantage of the open architecture and its many vulnerabilities.

[29] Air Force Doctrine Document (AFDD) 2-8, *Command and Control*, 1 June 2007, 3.
[30] AFDD 1, *Air Force Basic Doctrine*, 28.
[31] Lt Col Clint Hinote, *Centralized Control and Decentralized Execution* (Maxwell Air Force Base, AL: Air Force Research Institute, 2007), 61.

Militaries conduct operations in cyberspace at nearly the speed of light and the architecture of cyberspace is continually changing. Cyberspace is an ever-expanding domain with millions of new users and devices added annually.[32] Changing protocols, hardware, and software create new opportunities and vulnerabilities. All result in an operational environment where "offense is easy, and defense is difficult."[33]

Through cyberspace, commanders can control operations from extreme distances; expanding the possible battlefield to where conflict at a specific time and location no longer has meaning. The Air Force must fight and win a cyber conflict in several theaters simultaneously. The Secretary and Chief of Staff of the Air Force stated in a 20 August 2009 memo "every Airman must become a cyber defender, whether acting as part of a team or individually on Air Force networks. We must all conduct ourselves as "Cyber Wingmen."[34] Cyberspace forces are deployed on the ground in the most inhospitable of locations directly connected to services in the continental United States.

Summary

Why is command of cyber so important for the future of the Air Force? As President Obama recently stated, "Our technological advantage is key to America's military dominance. But our defense and military networks are under constant attack."[35] The Air Force has gladly assumed the moniker of the technological force. From a force originated by the invention of the technological miracle that allowed humans to fly, through the development of the intercontinental ballistic missile, to the launching and controlling of manned spacecraft, the Air Force has been at the forefront of technology. As the Air Force becomes further dependent on networks to conduct operations, the battle to control cyberspace will determine who wins the larger engagement.

---

[32] Internet Systems Consortium, "The ISC Domain Survey," https://www.isc.org/solutions/survey (accessed 24 May 2010).
[33] Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer et al. (Washington, DC: National Defense University Press, 2009), 272.
[34] Secretary of the Air Force and Chief of Staff, United States Air Force, Memorandum for all Airmen, 20 August 2009.
[35] President Barack Obama, "REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S INFRASTRUCTURE," *The White House*, 29 May 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed 11 February 2010).

DOD's recognition of cyberspace as a war-fighting domain provides the context required for cyberpower to reach its full potential. However, the DOD must be cautious of putting too much efficacy in theories of strategic information warfare or cyber warfare.[36] Warfare in cyberspace will require the services to integrate cyberpower into their existing competencies and develop strategies that take advantage of opportunities and diminish risks to achieve military objectives.

Chapter 1 will provide a history of command and control in the land, sea, and air domains and discuss how technology influenced the choices a commander made in planning and operations with respect to centralizing command and control and how this experience was carried forward. Chapter 2 will describe the command and control approach for the air, space, and cyberspace and demonstrate through a scenario how the different elements interact to control a time sensitive target event that traverses all three Air Force domains. Chapter 3 will compare and contrast the domains and provide recommendation on the best command and control approach for Air Force cyberspace. Finally, this paper proposes how the Air Force may best posture its forces to command and control the domain for a significant conflict.

The Air Force must not apply a command and control approach to cyberspace that is in conflict with the universal nature of war nor impede flexibility in response to the changing character of war.[37] The ultimate purpose of command and control of Air Force cyberspace is not the most efficient operation of the network, but to ensure it is available and useful to all airmen. Above all, it is crucial that the Air Force command and control cyberspace with a philosophy of enabling and enhancing the fight in the air and space to ensure success on the ground.

[36] David J. Lonsdale, *The Nature of Warfare in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 138-141.
[37] For a discussion of the nature and character of war, see Lonsdale, *Nature of War in the Information Age*, 28-43.

Chapter 1

History of Command, Control, and Communications

> *Historically, we communicators, with few exceptions, have not seen ourselves as part of the operational community. That is changing. Over the course of the next few years, we will become more integral to the fight than previously imagined. We are now engaged in the process of becoming so infused throughout the Air Force's operational community, that one day our now distinctive roles will be barely distinguishable.*
>
> *— Lieutenant General William J. Donahue*

Martin van Creveld writes in *Command in War*, "The problem of commanding and controlling armed forces, and of instituting effective communications with and within them, is as old as war itself."[1] As the size of armies grew, specialization and a general staff became necessary to oversee both mobilization and operations. Simultaneously, vastly improved communications technology allowed command and control over vast areas. Commanders now had the option to choose between centralized or decentralized control.[2]

Throughout history, the evolution of command and control and cyberspace has been conjoined in time and function. As the advancement of communications technology and computers has increased the ability of the commander to see the battle space and process information, they have been induced to further centralize control. However, centralization of control and better technology has not necessarily eliminated the friction of warfare that Clausewitz described almost two centuries ago.[3]

An analysis of the history of command and control can demonstrate how the strengths and limitations of communications technology have influenced commanders towards centralization or decentralization. In the nineteenth century, the development of general staffs became necessary to provide a means to understand an increasingly complex information environment. As the speed, range, and destructive potential of operations increased during the twentieth century, command and control increasingly

[1] Martin van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985), 1.
[2] Creveld, *Command in War*, 6.
[3] Carl Von Clausewitz, *On War*, ed. and trans Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 119.

became centralized.[4] However, the continuous improvement of technology, computerization, and the use of the space domain has created an ever more complex situation and pushed militaries towards network centric warfare.[5] The ubiquitous nature of communications technology has aggravated a long running conflict between retaining centralized control and the decentralization of decision-making enabled by shared battlespace awareness.[6]

Napoleonic Command

The French Revolution led a drastic change in the composition of armies from private ventures funded by a king to ones inspired by nationalistic and patriotic fervor. Spurred on by *levėe en masse*, the conscripted *Grand Armee* expanded beyond anything Europe had seen previously.[7] With operations soon extending over hundreds of miles, even a strategic genius such as Napoleon could not process and disseminate the amount of information to command and control forces in the field without some sort of structure.

As the head of state, Napoleon placed himself at the center of the command and control structure. Napoleon created subordinate organizations of armies and corps with the required staffs and support to operate independently, but were uniform in capability. Being interchangeable, the commander could deploy a corps' as the main effort in one engagement or as the supporting or reserve corps in the next.[8]

He then created the Imperial staff to collect and filter information from subordinate units for him to analyze.[9] The information provided through reports from informants, his staff, and corps commanders would sometimes become diluted through reinterpretations up the chain of command before it got to Napoleon.[10] To get a better picture of the actual situation, he could then direct what van Creveld calls the "directed telescope" at the "enemy forces, the terrain, or his own army" at the time and in the place

---

[4] C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven, CT: Yale University Press, 1990), 134.
[5] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed. (Washington DC: DoD C4ISR Cooperative Research Program, 1999), 2.
[6] Gregory A. Roman, "The Command or Control Dilemma: When Technology and Organizational Orientation Collide," Air Force 2025 study (Maxwell AFB, AL, Air University, 1996), 2.
[7] David G. Chandler, *The Campaigns of Napoleon* (New York, NY: Scribner, 1966), xliii.
[8] Creveld, *Command in War*, 61.
[9] Creveld, *Command in War*, 74.
[10] Creveld, *Command in War*, 75.

he desired.[11] Napoleon would then interpret this information and draft orders for his corps commanders to execute. For the first time, the commander did not have to be at the front to direct the battle.

When Napoleon took the field in the late eighteenth century, the communications technology was much as it was during the Roman Empire. With the exception of the semaphore telegraph and an improved road network, the same methods of communication used by Caesar were the methods Napoleon employed to direct the conquest of Europe. However, while this command and communications system worked initially, it broke down when the genius was not at the center of operations. As the campaigns grew in size, or too remote for Napoleon to control himself, it became apparent that although the corps was able to maneuver and execute operations, many corps commanders did not have the strategic acumen necessary for victory.[12]

The American generals of the Civil War studied Napoleon's tactics, but did not understand how the staff system was necessary to coordinate the large forces involved.[13] J.F.C. Fuller understood that "we can never guarantee that when war is declared we shall find a genius in control, we must create so perfect a piece of grand-strategical machinery that a man of normal intelligence and high training will be able to carry out the duties of grand strategy with effect."[14]

The Prussian General Staff and Decentralization

The Prussian chief of the General Staff from 1857-1887, General Von Moltke, wrote that, "No plan of operations extends with certainty beyond the first encounter with the enemy's main strength."[15] Moltke recognized the consequences increased size of armies, greater firepower, the railroads, and the telegraph would have on warfare and the need for "changes in strategy, tactics, command, and organization" to oversee the

[11] Creveld, *Command in War*, 75.
[12] Creveld, *Command in War*, 62.
[13] Although the Americans on both side of the Civil War studied Napoleon's tactics, they ignored the staff functions he established to enable the army to function. See Allard, *Command, Control, and the Common Defense*, 50.
[14] J.F.C. Fuller, *The Foundations of The Science of War* (London: Hutchinson & Co., LTD., 1926), 106.
[15] Helmuth von Moltke, *Moltke on the Art of War*, ed. Daniel J. Hughes (New York, NY: Ballantine Books, 1993) 45.

increased complexity of planning, mobilization, and deployment.[16] The Prussians developed an elite, professional group of staff officers selected for performance and trained in operational planning at the first staff college, the *Kriegsakademie*. These officers would gain both operational and staff experience by transitioning from field command to staff duty.[17]

The staff maintained an informal atmosphere with a free flow of ideas among the staff and the commanders in the field, which allowed the Prussians to react rapidly to evolving situations. The general staff officers maintained knowledge of current operations via reports and field visits, then utilized the information to modify plans and issue new orders based on the current situation.

Although having been employed in prior conflicts, the Prussians utilized the telegraph and railroad in an unprecedentedly effective way to conduct planning and the initial mobilization of forces.[18] Moltke wrote that the ability to send commands and receive reports from separate parts of the army "offers the means to direct separated parts of the army according to a single will toward a common goal."[19] He instructed future commanders to run telegraph lines as soon as practicable to all subordinate headquarters to maintain connectivity with the general staff.[20] Soon, the telegraph and railroad provided the instrument for the commander to direct forces and mobilize forces far from the headquarters. In the United States, Major Albert Myer convinced the US Army to create a separate, trained signal service in 1860. The telegraph became an instant command and control medium that was widely employed during the American Civil War.[21]

Similar to the situation in cyberspace today, the telegraph was no panacea to perfect communications; the Prussian technology was no better or worse than that available to the Austrians or the French.[22] Telegraph lines were easily disrupted, could

---

[16] Gunther E. Rotenberg, "Moltke, Schlieffen, and the Doctrine of Strategic Envelopment," in *Makers of Modern Strategy*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 299.
[17] Rotenberg, "Moltke and Schlieffen," 302.
[18] Creveld, *Command in War*, 104.
[19] Moltke, *Moltke on the Art of War*, 113.
[20] Moltke, *Moltke on the Art of War*, 113.
[21] Office of the Command Historian, "A Concise History of the U.S. Army Signal Corps," (Fort Gordon, GA: US Army Signal Center, 25 Jan 1994), 3.
[22] Creveld, *Command in War*, 107.

be tapped, and were not very mobile; making it imperative to be careful with the timing and type of information that was transmitted. Moltke stressed that the advantages the telegraph provided Prussian forces were also realized by the enemy, so efforts were to be made to locate the "constantly expanding underground telegraph lines…those which are behind enemy front—are to be destroyed."[23]

There was recognition that operational planning was necessary, but once the conflict began, flexibility, mobility, and the importance of providing subordinate commanders the freedom to react to the local situation would determine the victor and the vanquished.[24] As an Austrian officer wrote in 1861, "A commander who is tied down in this way is really to be pitied; he has two enemies to defeat, one in front and another in the rear… everything combines to rob the commander of his force and independence, partly by accident, partly by design. To prevent the telegraph from doing too much damage in war it is necessary either to have a great prince on the throne or a courageous commander with a strong character who, unafraid to assume responsibility, will know how to disregard a dispatch from home."[25] To cope with the difficulty of command in war, Moltke stressed the importance of issuing *Auftragstaktik*, mission-type orders, to subordinate commanders that would provide "definite tasks but not be limited in the choice of means to accomplish them."[26]

The telegraph and railroad greatly assisted planning and mobilization; however, it was less useful during maneuver and combat. The Prussians encouraged decentralized operations--once the armies deployed, no further attempt to control them was made.[27] For example, after the battle of Kőnnigrätz, Moltke wrote that the general staff and corps commanders had effectively lost command and control of the situation; it was only the initiative of the "battalions, or even companies" that secured the Prussian victory.[28] A thorough understanding of the overall plan was necessary for subordinate commanders to continue operations when the connectivity with the front was severed. The commanders in the field understood the commander's intent and could continue operations without

[23] Moltke, *Moltke on the Art of War*, 114.
[24] Moltke, *Moltke on the Art of War*, 133.
[25] Creveld, *Command in War*, 108.
[26] Moltke, *Moltke on the Art of War*, 156.
[27] Creveld, *Command in War*, 121.
[28] Creveld, *Command in War*, 140.

direction from the general staff. However, as communications technology continued to improve, these lessons were soon lost. Headquarters staffs increasingly attempted to employ more and extended control over front-line commanders.

Trend towards Centralization

The carnage of World War I occurred due to a stark lack of strategic leadership and the dramatic changes wrought by the industrial revolution. Armies of great size, equipped with unimaginable firepower created new challenges for commanders.[29] To deal with the incredible complexity of mobilizing, deploying, and committing such an intricate machine, most armies had adopted a form of the Prussian general staff. The huge increase in army size also saw a dramatic increase in the size of the staff to coordinate everything. To direct operations, both sides connected the headquarters staffs from corps to the brigade via telegraph and telephone.[30] Unfortunately, the headquarters had little understanding of the situation on the front and "the task of day-to-day management gained in importance to the point where it often over-shadowed the military side of things."[31]

The maneuverability Moltke employed to defeat the French resulted in the offensive form of warfare being interpreted as dominant when World War I began.[32] However, the dramatic increase in firepower without a matched increase in maneuver vaulted the defense to a dominant position and a strategic stalemate stagnated into trench warfare.[33] In relatively fixed positions, the signal units on both sides created an intricate network that grew at exponential rates. For example, the US Army Signal Corps grew quickly and alone built two hundred and seventy-three telephone exchanges and one hundred and thirty-four permanent telegraph offices connected by over 40,000 combat lines in less than two years.[34] A mindset of management over command developed

[29] Creveld, *Command in War*, 148.
[30] Creveld, *Command in War*, 169.
[31] Creveld, *Command in War*, 156.
[32] Alistar Horne, *The Price of Glory: Verdun 1916* (New York, NY: Penguin Books, 1993), 11.
[33] Michael Howard, "Men against Fire: The Doctrine of the Offensive in 1914," in *Makers of Modern Strategy*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 510-526.
[34] Office of the Command Historian, "A Concise History of the U.S. Army Signal Corps," 17.

where commanders employed industrial management techniques and utilized telephone connectivity to plan and direct operations far from the front.[35]

The British planning for the Battle of the Somme in 1916 was meticulous. Headquarters assigned corps specific goals, timelines, and maneuver areas.[36] The commander retained centralized control and gave little flexibility to subordinate commanders to press the attack, rather demanding they stay in contact and request permission from upper echelons.[37] Wireless communications were unreliable and too heavy to move forward, so commanders were reliant on a wired telephone system that was fixed and easily damaged during battle.[38] The situation resulted in British commanders, down to the battalion level, remaining in telephone boxes instead of commanding in the field and could provide neither proper command nor accurate information to higher headquarters.[39] The inability to move the telegraph or telephone lines during movement provided another advantage to the defense that fought from fixed positions, remained connected, and could centralize command and control.[40]

In contrast, although the Germans could be tempted by the same "telephonitis" as the British, they understood that confusion was the normal state of battle and wired communications were subject to disruption.[41] In the tradition of the Prussian general staff, they ensured a level of decentralization and lowering of decision authority while attempting to provide mutual support when required.[42] The armies of World War I successfully employed the telephone and telegraph to plan and mobilize massive forces, but communications technology still had not advanced to the point to allow centralized control of a mobile force, decentralization was still necessary.

In the end, information superiority resulted in a strategic victory for the Allies. The British had such superiority in global communications at the start of World War I that they were immediately able to sever the private telegraph lines out of Germany,

---

[35] Creveld, *Command in War*, 156-157.
[36] Creveld, *Command in War*, 161.
[37] John Keegan, *The Face of Battle* (New York, NY: Penquin Books, 1976), 218.
[38] Creveld, *Command in War*, 162.
[39] Martin van Creveld, *Technology and War: From 2000 B.C. to the Present* (New York, NY: The Free Press, 1989), 174.
[40] Creveld, *Command in War*, 186.
[41] Creveld, *Command in War*, 169.
[42] Creveld, *Command in War*, 169.

forcing them to rely on neutral lines for communication.[43] Soon after, the British began a systematic attack on the German radio relay stations, effectively cutting Germany off from strategic communications with neutral countries, including the United States. Because of the isolation, Germany had to encrypt the message traffic that would travel through London. The British intercepted the "Zimmerman telegram" from the Germans foreign office to the Mexican government imploring them to initiate an attack on the United States.[44] With the capability to decrypt German messages, the British passed this information to the Americans, persuading them to join with the Entente Powers and turn the tide to defeat Germany.[45]

Sea power also saw a transformation in the early twentieth century from a naturally decentralized command and control philosophy to one increasingly centralized. Historically, once naval vessels departed they were without contact or subject to control by higher command. Based on the influence of Alfred Mahan's seminal work, *The Influence of Sea Power upon History*, the United States embarked to remake itself as a formidable sea power at the same time communications technology was making advancements. Building twenty-thousand ton battleships with integrated fire control systems and reliable wireless communications extended the range a fleet commander could effectively control his forces.[46] The long-range communications stations constructed on shore to coordinate the movements of US naval vessels were capable of intercepting and decoding enemy messages. The ability to decipher enemy submarine locations and control friendly forces was critical to enabling effective deployment of destroyer screens across the Atlantic.[47]

Airpower played a relatively minor role in World War I where reconnaissance and artillery spotting were the primary functions of the airplane. With few exceptions, the United States decentralized the command and control of airpower to ground commanders

[43] Peter J. Hugill, *Global Communications Since 1844: Geopolitics and Technology* (Baltimore, MD: John Hopkins University Press, 1999), 46.
[44] Hugill, *Global Communications Since 1844*, 47.
[45] Hugill, *Global Communications Since 1844*, 48.
[46] Allard, *Command, Control, and The Common Defense*, 69.
[47] Allard, *Command, Control, and The Common Defense*, 83.

and allowed them to direct the areas to be searched.[48] To provide information quickly to the ground commanders, the Aviation Section of the US Signal Corps installed primitive wireless radio sets in the planes, but by the end of the war, the radios had become quite sophisticated.[49] The development of the airplane and wireless technologies would advance rapidly and play a much more vital role in World War II.[50]

The telephone and telegram tempted World War I commanders to centralize command and control and worked well in fixed defensive positions. However, the technology was not reliable or mobile enough to allow centralized control of maneuver warfare required to go on the offensive. The inability to see the battlefield, yet keep subordinate commanders tied to fixed telephones effectively froze any possible advance.

Mobility and Decentralization

Technological innovation proceeded rapidly in the interwar period. The airplane, radar, and radio had matured enough to become extremely effective on the battlefield. World War II saw offensive strategies once again become dominant, where firepower, speed, and reliable radio communications made it possible to coordinate forces over a wide area to out-maneuver defensive forces. In the air, the Germans and British each created separate air services and the Americans gained some independence by establishing the Army Air Corps. Inspired by the writings of Gulio Douhet and Brigadier General William Mitchell, the American and British air forces adopted a decidedly offensive strategy to eliminate the enemy's ability to wage war by attacking industry and infrastructure.[51]

In rapid fashion, the German panzer divisions vanquished armies that had locked on to the defensive strategy of the past war. Fixed defenses were unable to match the highly decentralized German *blitzkrieg* tactics whose chain of command relied on

---

[48] Daniel R. Mortensen, "The Air Service in the Great War," in *Winged Shield, Winged Sword, Volume I*, ed. Bernard C. Nalty (Washington DC: United States Air Force, 1997), 40. Also see Lee Kennett, *The First Air War: 1914-1918* (New York, NY: Free Press, 1991), 87.
[49] Hugill, *Global Communications Since 1844*, 149.
[50] Williamson Murray, "Strategic Bombing: The British, American, and German experiences," in *Military Innovation in the Interwar Period*, ed. Williamson Murray and Allan R. Millet (New York, NY: Cambridge University Press, 1998), 98. For an excellent history of the US Air Force and the advancement of air power, see *Winged Shield, Winged Sword, Volume I*, ed. Bernard C. Nalty (Washington D.C.: United States Air Force, 1997) 231-268.
[51] Richard J. Overy, *The Air War, 1939-1945* (Washington, DC: Potomac Books, Inc., 2005), 64.

"intelligent initiative at every rank, beginning with the lowest, in order to seize every fleeting opportunity and exploit it to the hilt."[52] The advancement of radio technology made it possible for the higher headquarters to maintain a semblance of control and coordinate divisions towards the overall plan. It is not surprising that one of the creators of armored command, Heinz Guderian, was a signals officer in World War I.[53]

The British fear of strategic bombing incited political demand to create an intricate home radar defense system. By 1939, there were twenty-one Chain Home radar stations circling the island, connected to command headquarters by an efficient system of landlines.[54] In conjunction with intercepted German radio transmissions from in route aircraft, the British integrated signals intelligence with the radar picture to provide a clearer estimate of where the attack would take place.[55] The system demanded strict adherence to procedure, rapid reporting, and clear direction to group and sector defense systems to be effective. Once the headquarters determined who was to respond, the fighters in the air took over the tactical engagement.[56]

Much of the German Luftwaffe remained closely tied to the tactical support of ground forces. As early as 1937, the Luftwaffe had identified radar-tracking systems as "urgent and critical importance," yet the "Luftwaffe proved ambivalent in its pursuit of this new technology, most likely a result of its demonstrated penchant for weapons with offensive rather than defensive applications."[57] By 1940, the Germans had created a chain of radar stations on the north coast of Europe, but the system lacked integration. The German radars were as technologically advanced as the British radars, but they lacked a centralized command and control system to connect the radars, flak, and fighter commands; resulting in a system less effective than might otherwise have been possible. The combined influence of Nazism that discouraged centralization and the overarching offensive strategy retarded the development of a centralized command and control air

[52] Creveld, *Command in War*, 191.
[53] Creveld, *Command in War*, 192.
[54] Richard J. Overy, *The Battle of Britian* (New York, NY: W.W. Norton & Company, Inc., 2002), 44.
[55] Overy, *Battle of Britian*, 46.
[56] Michael W. Kometer, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower* (Maxwell Air Force Base, AL: Air University Press, 2007), 43.
[57] Edward B. Westermann, *Flak* (Lawrence, KS: University Press of Kansas, 2001), 70.

defense system to defend Germany until much later in the war. By then it was too late to recover.[58]

Airmen have long advocated for centralized control of air forces to take advantage of airpower's inherent flexibility. During World War I, although most airpower was in direct support of ground operations, American Colonel William Mitchell pioneered centralized control of airpower by unifying the efforts of 1,481 French and American aircraft under his direct command in the attack on the Saint Mihiel salient.[59] However, World War II saw disaster for the Allies at Kasserine Pass in North Africa when they decentralized control and divided airpower between the ground commanders. Treated as flying artillery, the ground commanders underutilized the aircraft available and attacked inconsequential or low payoff targets.[60] In response, the US Army Air Corps clearly stated in the 1943 version of FM 100-20, "the inherent flexibility of air power is its greatest asset…control of available air power must be centralized and command must be exercised through the air force commander if this inherent flexibility and ability to deliver a decisive blow are to be fully exploited."[61] As the war continued, the Allies employed airpower in a variety of roles and command relationships.

To prepare for Operation OVERLORD, the invasion of Europe, the Allies decentralized some level of control of tactical air forces by encouraging their fighters to search for and attack transportation targets as they were discovered.[62] By sending thousands of fighters on search and destroy missions "in the two weeks before the invasion, these Chattanooga CHOO-CHOO missions claimed 475 locomotives and cut rail lines in 150 different places."[63]

World War II saw two styles of command and control gain success. British air defenses were highly centralized and defensive, while German panzer and American tactical air force operations were decentralized and employed an offensive strategy. The

---

[58] Overy, *Air War*, 202.
[59] John H. Morrow, Jr., *The Great War in the Air, Military Aviation from 1909 to 1921* (Tuscaloosa, AL: The University of Alabama Press, 1993), 337.
[60] Major Shawn P. Rife, "Kasserine Pass and the Proper Application of Airpower," *Joint Force Quarterly*, Autumn/Winter 1998-99, 77.
[61] War Department Field Manual 100-20, *Field Service Regulations, Command and Employment of Air Power*, 21 July 1943, 1.
[62] Thomas A. Hughes, *OVER LORD: General Pete Quesada and the Triumph of Tactical Air Power in World War II* (New York, NY: The Free Press, 1995), 129.
[63] Hughes, *OVER LORD*, 130.

combined strategic bombing offensive was highly centralized in order to plan, schedule, and identify the specific targets.[64] This dichotomy of the bombing offensive may help explain why the overall effectiveness of the American and British efforts remains unclear. The information to determine what targets would be most effective targets to hit and the technology to attack accurately those targets selected did not exist.[65] There is little doubt that when the air efforts to prepare for Operation OVERLORD demanded the decentralization of tactical airpower in an offensive role to strike targets as they became available, it was very successful.[66] In any case, it is obvious that the centralization or decentralization of command and control must be grounded in the environment, mission requirements, and consequences of action.

The command and control of airpower during Vietnam suffered significant problems. The Air Force's command and control element, the Tactical Air Control Center (TACC) improved the commander's situational awareness; however, the presentation of information remained remarkably stagnant.[67] In addition, service parochialism fragmented the command and control of airpower between the Navy and the Air Force. Internally, the Air Force further fragmented airpower between Seventh Air Force control of tactical air forces in theater and Strategic Air Command in the United States centrally controlling strategic air forces. The challenges of planning missions from around the world and "a general culture that placed predictability over innovation" created plans that the theater air forces felt were tactically unsound.[68]

After considerable issues with command, control and communications during the joint operations in Iran and Grenada, the Goldwaters-Nichols Act of 1986 established the regional Combatant Commanders as the commanders of all US military forces in their area of responsibility.[69] It also established the tenet that the senior airman in theater would be the Joint Force Air Component Commander (JFACC), who would centralize control and recommend apportionment of airpower to the Joint Force Commander (JFC).

---

[64] Bernard C. Nalty, "The Defeat of Italy and Germany," in *Winged Shield, Winged Sword, Volume I,* 281.
[65] Overy. *Air War*, 110-111.
[66] Hughes, *OVER LORD*, 131.
[67] Kometer, *Command in Air War*, 44.
[68] Kometer, *Command in Air War*, 40.
[69] Kometer, *Command in Air War*, 87.

The first real test of the responsibilities of a JFACC came during the Gulf War. Although disagreements persisted between services on the actual authorities of the JFACC to control inter-service airpower, the JFC gave US Air Force Lieutenant General Charles Horner responsibility to plan and coordinate the air portion of the campaign.[70] This authority allowed a greater degree of coherence in the planning and conduct of air operations than would have occurred if the Navy and Air Force were assigned separate operating areas as in Vietnam.[71]

Space War

The immediate geo-political situation after World War II demanded the United States maintain an active military larger than had historically been the norm. The National Security Act of 1947 created the US Air Force to address the recognized importance of the air domain. Technology advanced rapidly during and in the aftermath of World War II; the first atomic weapon was deployed in 1945; the first electronic digital computer was built in 1946; and the first intercontinental ballistic missile launched in 1957.[72] Together, these events have had a profound effect on the speed and range of military operations and command and control requirements. The rapid advancements in communications technology enabled centralization in all war-fighting domains.[73] To prevent escalation of limited conflicts into an unlimited war, which neither the United States nor the Soviets wanted, the highest levels of government retained some level of centralized control over both nuclear and conventional military forces.[74]

The advent and proliferation of nuclear weapons demanded that both nations develop and maintain highly centralized command and control systems that had multiple checks and balances on their employment. Due to the extreme consequences of employing nuclear weapons, commander's initiative was not allowed, nor was it realistic

[70] Diane T. Putney, *Airpower Advantage: Planning the Gulf War Air Campaign 1989-1991* (Washington DC: United States Air Force, 2004), 347.
[71] Putney, *Airpower Advantage*, 4-6.
[72] Walter A. McDougall, *…The Heavens and The Earth: A Political History of the Space Age* (Baltimore, MD: The Johns Hopkins University Press, 1985), 4-11.
[73] Allard, *Command, Control, and the Common Defense*, 134.
[74] Allard, *Command, Control, and the Common Defense*, 134.

to expect restricted use of nuclear weapons at the tactical level of war.[75] Because of the fear of escalation, the conflicts in Korea and Vietnam demanded restraint with respect to the weapons employed and the limited objectives sought.

The Cold War was a superpower struggle between two competing economic systems conducted partially through a proxy war termed the "space race." In an effort to enhance national prestige and demonstrate whose system was best, the US and Soviet space programs represented each nation's technical and economic strength.[76] The race was the impetus behind the competition in space programs and the proliferation of the intercontinental ballistic missile. The United States and Soviets quickly adapted the same missile technology used to deliver nuclear weapons to launch reconnaissance and communications satellites that could provide both the ability to control forces globally and awareness of enemy capabilities.

The benefits of computerization of telecommunications and the requirement to maintain contact with nuclear forces around the world soon extended to the conventional forces. On 18 December 1958, the United States launched the first communications satellite, Project SCORE (Signal Communications via Orbiting Relay Equipment), to prove that messages could be sent from the ground to space, stored, and then retransmitted to the ground.[77] Vietnam saw the first use of satellite communications in combat via the experimental synchronous communications satellite, known as SYNCOM, in 1966.[78] SYNCOM provided one voice circuit and one data circuit to Hawaii and became a critical mechanism for US commanders in Vietnam to communicate with Washington D.C.[79] The Pentagon also established the Defense Communications Agency and the Worldwide Military Command and Control System to allow coordination with on-scene commanders throughout the world.[80] These capabilities made it easy for

[75] For an excellent discussion on the development of American Nuclear Security Strategy see Campell Craig, *Destroying the Village: Eisenhower and Thermonuclear War* (New York, NY: Columbia University Press, 1998).
[76] Michael Sheehan, *The International Politics of Space: No Final Frontier* (London: Routledge, 2007), 20.
[77] Command Historian, "A Concise History of the U.S. Army Signal Corps," 26.
[78] David N. Spires, *Beyond Horizons: A Half Century of Air Force Space Leadership* (Maxwell AFB, AL: Air University Press, 1998), 170.
[79] Command Historian, "Concise History of the U.S. Army Signal Corps," 28.
[80] Allard, *Command, Control, and The Common Defense*, 136.

civilian leadership in the pentagon to bypass the normal chain of command in exchange for unfiltered information.

The Gulf War also saw the space domain become instrumental to US dominance on the battlefield. The United States had developed and deployed satellites with multiple military support capabilities including navigation, weather, missile defense, and several types of communications satellites. The effect of all these capabilities was an unprecedented capability to monitor ongoing operations from the TACC and centralize the command and control of forces by transmitting taskings to more than 1,500 deployed satellite terminals in order to coordinate airpower throughout the theater of operations.[81] Shortly after the Gulf War, The Air Force recognized the critical importance of the AOC to effective command and control of air operations and renamed the TACC the Air Operations Center (AOC). To ensure the proper funding, training, and reliable communications architecture, the Air Force certified the command center as a weapon system in 2000.

Network Centric Warfare

The advancement of computer and communications technology has dramatically enhanced the military commander's ability to command and control their forces. Transformative command and control systems have shaped doctrine and become integral to the weapon systems modern Air Forces employ. As the proliferation of computers and digital communications dramatically increased at the tactical level, decision cycles became compressed. As professed by Air Force Colonel John Boyd through the use of the Observe-Orient-Decide-Act, or OODA loop, the speed at which one could orient to the combat situation would most likely determine the winners and losers.[82] In the air, land, and sea domains, automation of weapons systems allowed the processing of battlefield information to provide decision recommendations to operators.

A complex network of tactical data links on multiple aircraft platforms provided the AOC with an unprecedented picture of the battle space. Soon, almost every aircraft became a sensor for the network. The purpose of the data links was to share data

[81] Spires, *Beyond Horizons*, 256.
[82] Grant T. Hammond, *The Mind of War: John Boyd and American Security* (Washington, DC: Smithsonian Books, 2001), 162-167.

between sensors to speed decision cycles by promoting self-synchronization. As the number of sensors in the network increased, and the picture at the AOC became more complete, timely, and accurate, the temptation increased for the AOC to intervene in current operations. After all, if the AOC has the best information and the "complete" picture of the battle space, should not the JFACC centralize important decisions? However, it may be dangerous for commanders to be involved with tactical decisions, which could result in the commander being unable to form a holistic view of whether the strategy is working and risks disempowering tactical units to a point where they do not innovate or they ignore headquarters directives.[83]

The expansion of satellite communications, secure, and non-secure data networks put information closer to the user in the field and extended the commander's ability to communicate with their forces. The Global Positioning System (GPS) provided previously unforeseen capacity to know where forces were on the battlefield. GPS proved invaluable and was an asymmetric advantage to US ground maneuver forces during the Gulf War as they navigated across the open desert.[84] In the mid-1990s, the ability to drop munitions guided by GPS receivers revolutionized the accuracy and collateral damage expectations of the Air Force. The most popular type of GPS guided weapon, the joint direct attack munition (JDAM), became critical during Operation Allied Force, where so many were employed the Air Force almost ran out.[85]

With GPS and improved satellite communications, pilots could now control Remotely Piloted Vehicles (RPV) globally due to the combination of satellite communications and GPS. This process continues with the force slowly transforming from a force built around bomber and fighter pilots to one heavily reliant on RPVs to conduct intelligence, surveillance, reconnaissance, close air support, and information operations. For example, use of RPVs by the Army and Air Force has increased dramatically in Iraq and Afghanistan from 167 in 2001 to 5,500 by 2009.[86]

---

[83] Kometer, *Command in air war*, 180.
[84] Michael Russel Rip and David P. Lusch, "The Precision Revolution: The Navstar Global Positioning System in the Second Gulf War," *Intelligence and National Security*, Vol. 9, No. 2, April 1994, 171.
[85] Rip and Lusch, "The Precision Revolution," 238.
[86] Christopher Drew, "Drones Are Weapons of Choice in Fighting Qaeda," *The New York Times*, 16 Mar 2009, http://www.nytimes.com/2009/03/17/business/17uav.html (accessed Feb 9, 2010).

Ground forces extended GPS's utility to the individual soldier or vehicle via systems such as Blue Force Tracker (BFT). BFT provided commanders the unprecedented capability to track units across the theater. Benefits range from controlling movements, locating units in distress, and preventing fratricide. Eventually the Army plans to field the capability "to nearly 200,000 platforms and dismounted soldiers."[87]

All of this information was driving a determinate change in the possibilities of command and control. No longer was centralized versus decentralized command and control philosophy sufficiently descriptive to describe the information dense environment where speed and self-synchronization were required to operate. Network centric warfare could connect the political leaders, commanders, sensors, and shooters to translate information superiority into combat power.[88] Lieutenant General Tom Hobbins described how network centric warfare is not just for conventional operations.

> What will network centric warfare look like? Imagine a battle-space where every platform automatically sends all its critical data, machine-to-machine, through a network of ground-, air-, and space-based relays, protected by multilayer security, to the appropriate command centers where planners, analysts, and commanders see real-time depictions of the status of those units. The information does not come to the commanders raw but with intelligence fused and machine-processed to create decision-quality options for the decision makers. This "human in the loop" ensures that analysis takes place and turns information into actionable intelligence. Information and data are not useful until someone thinks about them, especially in combat where missing data is the norm. We need clear thinking. We certainly want speed of transmission, but we also want to transmit quality information. Once that process is complete, commanders make their decisions, and the results are again sent—machine-to-machine—to the affected units, which read and execute their orders and then generate more feedback to the command centers, thus driving further data sharing and awareness-based decisions. That is network centric warfare—and that is where we are going.[89]

[87] US Army Project Manager, Force XXI Battle Command Brigade and Below website, http://peoc3t.monmouth.army.mil/fbcb2/fbcb2.html (accessed 5 May 2010).
[88] Alberts, et al., *Network Centric Warfare*, 2.
[89] Lt Gen William Thomas Hobbins, "Airmen on the Battlefield," *Air and Space Power Journal*, vol. XIX, no. 1(Spring 2005), 68.

The use of information technology for command and control had taken a decidedly deterministic path. As network centric warfare continued to pervade all services and weapon systems, the decision cycle was perpetually shrinking as both speed and range increased dramatically. The network had now become so important to success that it had become a center of gravity, enabling operations versus merely enhancing effectiveness or improving commander cognition. Access and denial of information and the electro-magnetic spectrum had become a form of warfare. Out of the Myer's Signal Corps the Air Force was born, now cyberpower was again giving birth to a new domain of warfare. The command and control of that new domain presents new challenges for the Air Force.

Chapter 2

Command and Control of Air Force Operations

The differences in range, flexibility, and perspective with respect to surface warfare require a different approach to the application of air and space power. This outlook—the Airman's perspective—demands that Airmen understand and apply the distinctive characteristics of air and space power in a complex joint environment that is experiencing profound technological change.

— Air Force Doctrine Document 2

Space is no longer just the high ground; it is an integral part of the Joint fight. Today, space capabilities are embedded in a complex of systems that serve forces and commanders at every level and that span the spectrum of diplomatic, informational, military, and economic activities. And they do this from peace through crisis and war. Today, in Air Force Space Command, we are clearly active participants in the Joint fight that we are waging in overseas contingency operations. The capabilities we present have shaped the American way of warfare.

— General C. Robert Kehler

The history of command and control demonstrates how the advancement of communications technology greatly influenced the approach commanders employed in controlling their forces. New connectivity and situational awareness provided not only commanders, but also national leadership, the capability to see the battlefield and retain decision-making authority. The Air Force has attempted to harness these capabilities and utilize them to improve the command and control of air, space, and cyberspace forces.

The United States Air Force organizes, trains, and equips forces to assume the role of the lead service for the air and space domains, and has significant capabilities in the cyberspace domain. How the Air Force organizes forces and provides command and control of its forces varies in each war-fighting domain. These differences are driven by the unique physical characteristics of the domains themselves and the necessity to coordinate with joint, coalition, interagency, and civilian agencies for mission accomplishment.

Air Force Organizations for Command and Control

According to JP 1-02, command is "the authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions."[1] Command is a military designation distinguished from management by legal authority and the extreme consequences of military action.

Centralized control and decentralized execution are the Air Force's key tenets of command and control of air power.[2] The purpose of control is to optimize the force at the right time and place to ensure mission success. Centralized control provides the commander the ability to "exploit the speed, flexibility, and versatility of global air and space power" to achieve effects across the theater "when and where desired."[3] Centralized control of airpower ensures unity of effort and enhances effectiveness; in contrast to squandering opportunities and assets by dividing the control among separate commanders. Where centralized control achieves flexibility and versatility at the operational and strategic levels of war, decentralized execution attempts to foster initiative and retain flexibility at the tactical level of war where the airman on the scene can best take advantage of emerging opportunities.[4] To effectively execute centralized control, the Joint Force Commander (JFC) must designate a single commander to direct theater air forces.

The Air Force organizes, trains, and equips to support the requirements of the geographic combatant commanders (GCC) in air, space, and cyberspace. Over a century of flight history, armed forces have experimented with multiple approaches to command and control of air forces;[5] while the DOD has recognized space as a separate domain for just a quarter of a century and the structure for command and control of cyberspace has

---

[1] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 (amended 31 October 2009), 101.
[2] Air Force Doctrine Document (AFDD) 2-8, *Command and Control*, 1 June 2007, 12.
[3] AFDD 2-8, *Command and Control*, 12.
[4] AFDD 2-8, *Command and Control*, 15.
[5] For a discussion of the history of the tension between centralization and decentralization in commanding air forces see Lt Col Clint Hinote, *Centralized Control and Decentralized Execution* (Maxwell Air Force Base, AL: Air Force Research Institute, 2007), 7.

just recently been addressed. An analysis of the development and current command and control approach in the air and space domains compared to how the Air Force proposes to command and control Air Force cyber forces can provide options and may suggest the most appropriate organizational and operational approach. A case study of how the Air Force executes a time sensitive target (TST) for a joint force commander (JFC) can demonstrate the command and control of air, space, and cyber forces and the doctrinally "correct" operation of the command and control centers is affected by the unique environment, the character of conflict, and force structure of each domain.

Figure 2 lists the Air Force's seventeen key operational functions that it can present to the joint task force.[6] The prodigious advancements in air and space power provide the capability to conduct operations globally in support of multiple GCCs and across the entire theater of operations. However, air forces are in high demand but limited in number, and have the ability to respond to events in multiple theaters simultaneously. Also, the number of aircraft and required support forces limits the amount of missions that can be flown in a certain period of time. Likewise, a satellite can only be over one area of the earth at a time. With multiple requests for use of these limited assets, the optimum organization and command and control approach is necessary to wield the maximum air and space power possible across the multiple theaters.

Figure 2: Air & Space Power Functions
Source: Air Force Doctrine Document 1, *Air Force Basic Doctrine*, 17 November 2003

[6] Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, 17 November 2003, 39.

The GCC will retain or assign a subordinate joint force commander (JFC) to direct joint operations in a theater. Air Force doctrine advocates for the unity of command of air and space forces under a single commander; that air forces should not be divided among separate component commanders; and that centralized command and control is necessary to realize airpower's ability to provide effects on a theater and global scale.[7] The JFC will normally assign the role of joint force air component commander (JFACC) to the senior airman in theater.

The Air Force organizes, trains, and equips to execute JFACC responsibilities during joint and combined operations. The JFACC is normally also assigned the role of the area air defense commander responsible for defense of the airspace in the joint operations area (JOA); and the airspace control authority responsible to plan and de-conflict airspace in time and place.[8]

Air Force doctrine professes that due to the speed, range, and global capabilities of air forces, it is necessary to have a centralized command, planning, and control process.[9] Centralizing control of air power provides "the broad, strategic perspective necessary to balance and prioritize the use of a powerful, highly desired yet limited force."[10] To accomplish the multitude of tasks associated with the diverse roles of the JFACC, the Air Force has a robust command and control system called the theater air control system (TACS).

The senior element in this structure is the air and space operations center (AOC); in a coalition, it is referred to as the combined AOC, or the CAOC. The AOC is a highly centralized command and control node supported by a multitude of sensors, systems, and experts to monitor and direct the aircraft in theater. The amount of personnel and technological resources necessary to control air power across a theater is substantial. In fact, "the main reason lower-echelon air commanders cannot command and control airpower is that they lack the ability to do so."[11] The technology exists to push

[7] AFDD 2-8, *Command and Control*, 12.
[8] Joint Publication 3-30, *Command and Control for Joint Air Operations*, 12 January 2010, II-3.
[9] AFDD 2-8, *Command and Control*, 12.
[10] AFDD 1, *Air Force Basic Doctrine*, 28.
[11] Michael W. Kometer, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower* (Maxwell Air Force Base, AL: Air University Press, 2007), 59.

information to lower-echelons in the TACS, however, the additional costs must be balanced with the flexibility and tempo required of the operational environment.[12]

Figure 3 represents how the JFACC achieves unity of effort via horizontal and vertical integration with the headquarters, other component commanders, global air forces represented by the functional AOCs, and subordinate command and control organizations. The JFACC may establish air component coordination elements (ACCE) with the other component headquarters "and with the JTF to better integrate air and space operations within the overall joint force."[13] The other service components place specially trained liaison elements within the AOC to coordinate air and space operations. The AOC in conjunction with the liaison elements work with air support operations centers (ASOC) and tactical air control parties (TACP) operating in close proximity with ground forces to coordinate air support for ground operations.

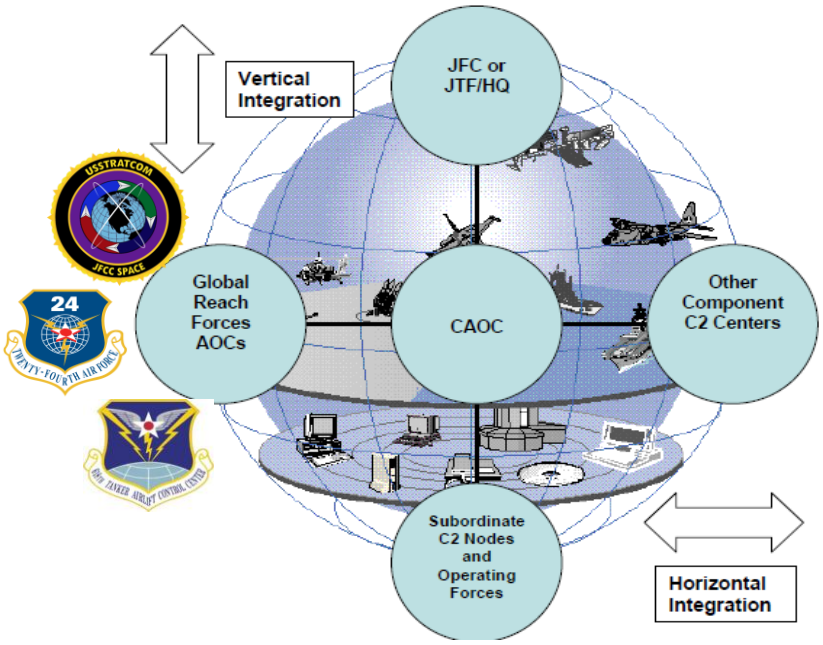

Figure 3: Information Integration
Source: Air Force Doctrine Document 2-8, *Command and Control*, 1 June 2007

[12] Lt Col Hinote proposes that limited resources require some degree of centralization at the strategic and operational levels of war, but decentralization at the tactical level allows for major gains in flexibility and tempo. *Centralized Control and Decentralized Execution* , 69-70.
[13] Air Force Doctrine Document 2, *Operations and Organization*, 3 April 2007, 71.

Command and Control of Air Power

A contemporary mission thread can best demonstrate how centralized control and decentralized execution of air power works in practice. The JFACC takes direction from the JFC and creates a plan for the theater's air assets to meet the JFC objectives. Figure 4 represents how the JFACC implements a typical 72-hour planning cycle. This process ensures the JFC's intent, priorities, guidance, and objectives are incorporated into the planning process, promulgated to the forces, executed, and assessed. This process results in orders from the AOC to joint air forces in the form of an air tasking order (ATO) and the airspace control order (ACO). While most missions are pre-planned, the JFACC diverts some missions during the execution portion of the ATO cycle to take advantage of emerging opportunities.

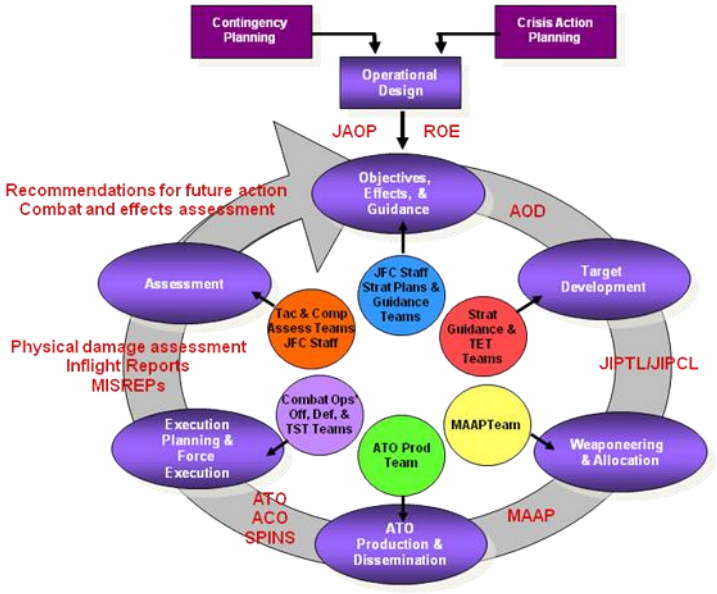

Figure 4: Joint Air Tasking Cycle
Source: Air Force Doctrine Document 2-8, *Command and Control*, 1 June 2007

A TST is a "JFC designated target or target type of such high importance to the accomplishment of the JFC's mission and objectives or one that presents such a significant strategic or operational threat to friendly forces or allies, that the JFC dedicates intelligence collection and attack assets or is willing to divert assets away from

other targets in order to find, fix, track, target, engage, and assess it/them."[14] TSTs are nominated targets of opportunity that may occur during the normal ATO cycle. The Air Force has continued to make progress in reducing the time it takes to respond to a TST, reducing the time to minutes if available assets are close to the target.[15] TSTs can cause tension among different levels of command when the operational command center asserts its authority to direct tactical execution.

The current operations division (COD) of the AOC orchestrates the TST process and executes TSTs in coordination with other components in the JTF. The COD provides constant monitoring of air missions under control of theater air control system and adjusts the ATO as necessary, for example, "when assigned targets are no longer valid, high priority targets are detected, or enemy action threatens friendly forces."[16]

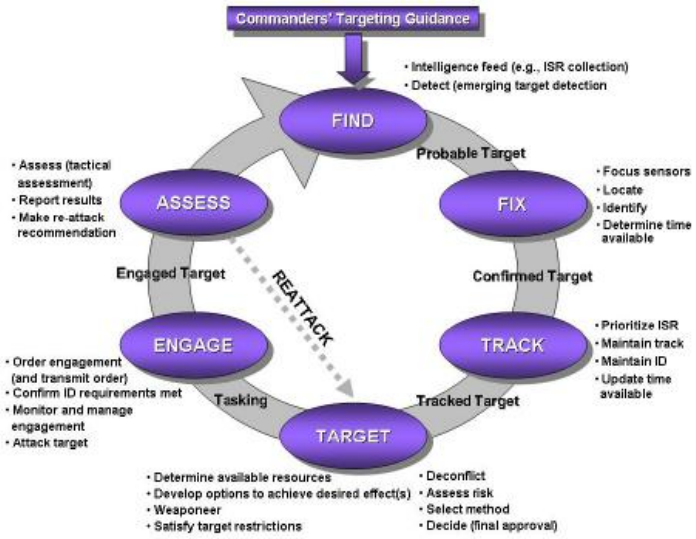

Figure 5: The Dynamic Targeting Process
Source: Air Force Doctrine Document 2-1.9, Targeting, 8 June 2006

The Air Force follows a six phase dynamic targeting process to execute TSTs: the phases are Find, Fix, Track, Target, Engage, Assess, or F2T2EA, shown in Figure 5. A complex process, it limits the amount of TSTs that can be coordinated at one time. Detailed rules of engagement (ROE) can speed the process and delineate what level of

[14] Joint Publication (JP) 3-60, *Joint Targeting*, 13 April 2007, I-5.
[15] Kometer, *Command in Air War*, 59.
[16] 505th Command and Control Wing, *C/JFACC Processes* (Hurlburt Field, FL, USAF Senior Mentor Training, September 2007), slide 34.

command can approve a TST. Obviously, the higher-level or more centralized the decision authority, the longer the process and fewer TSTs can be processed.

The first phase in the TST process is detecting a possible target. This is typically accomplished by an intelligence, surveillance, and reconnaissance (ISR) platform detecting the potential TST and reporting to the AOC. The COD immediately begins to validate the target against ROE and the JFC's guidance. Meanwhile, the target is fixed utilizing multiple platforms including the global positioning system (GPS) to provide the location of the target location to the AOC. We shall consider a specific case where the fixing is done with mensurated coordinates to facilitate precise weapons. Sensor networks and ISR platforms connected via satellite communications or line of site radio links continue to track the TST during coordination with the other components and coalition forces to deconflict the battle space and conduct risk assessment. If a weaponized remotely piloted vehicle (RPV) detects the target, the ISR platform may be the same that engages.[17]

Once the AOC positively confirms the identity of the target and validates the applicable criteria, they select the most appropriate weapons platform to execute the attack. The engagement decision is made at the appropriate decision level according to the ROE and the targeting data is transmitted to the tactical command and control nodes for decentralized execution of the actual engagement and continued monitoring. Finally, a post-strike battle damage assessment is conducted to determine required follow on actions.

The preceding TST process demonstrates the competing demands of centralized control of operations, target approval by the JFC or even national leadership, and the rapidity of decentralized finding and engaging portions of the TST process. The ability to centralize control of aircraft or other assets capable of targeting the TST is necessary for both flexibility and responsiveness. The centralized approval of targets is necessary to ensure that they are worth diverting assets from pre-planned targets, are in synch with JFC objectives, and the strategic implications are considered with respect to collateral damage and first, second, and third order effects. However, over-centralization can result in missed opportunities and limit the number of TSTs the AOC can execute. Therefore,

[17] Air Force Doctrine Document (AFDD) 2-1.9, *Targeting*, 3 June 2006, 51.

"placing the appropriate level of battlespace awareness at subordinate command and control nodes can streamline the command and control cycle and allow timely engagement during dynamic targeting."[18] In addition, improved situational awareness systems, an open information architecture, and the maturation of network-centric operations can allow decentralized coordination to more quickly execute TSTs.

Command and Control of Space Operations

Space power provides a significant asymmetric advantage for US forces. This advantage demands that the United States maintains space superiority through space control at all times. The space domain is both a critical piece of the cyberspace domain and heavily reliant on portions of cyberspace to operate and provide effects to the GCCs. While air forces are typically assigned to a GCC, the "Unified Command Plan establishes USSTRATCOM as the functional unified command with overall responsibility for military space operations. CDRUSSTRATCOM, has combatant command (COCOM) command authority of all space forces as assigned by the SecDef in the *Forces For Unified Commands* memorandum. CDRUSSTRATCOM employs these forces to support worldwide operations."[19] The command and control of Air Force space forces requires a different approach than the command and control of air forces. The global nature of the space domain and the limited number of space forces means they must be allocated intelligently through a highly centralized command and control structure.

Space power provides valuable force enhancement and force application services to the joint force commander through weather monitoring, satellite communications, ISR, missile warning, and precision, navigation, and timing (PNT) services. As with air power, Air Force doctrine posits that the global nature of space power is best employed when placed under the command of a single airman.[20] Command and control of space forces can be very difficult because the Air Force must integrate military space assets with many non-military space assets to support military operations.

The Fourteenth Air Force commander under Air Force Space Command serves as the CDR JFCC-Space. A functional AOC called the Joint Space Operations Center (JSpOC) provides the command and control node to direct global military space forces.

[18] AFDD 2-1.9, *Targeting*, 53.
[19] Air Force Doctrine Document (AFDD) 2-2, *Space Operations*, 27 November 2006, 10.
[20] AFDD 2-2, *Space Operations*, 3.

During most operations, space forces are in general support of the geographic combatant commanders.

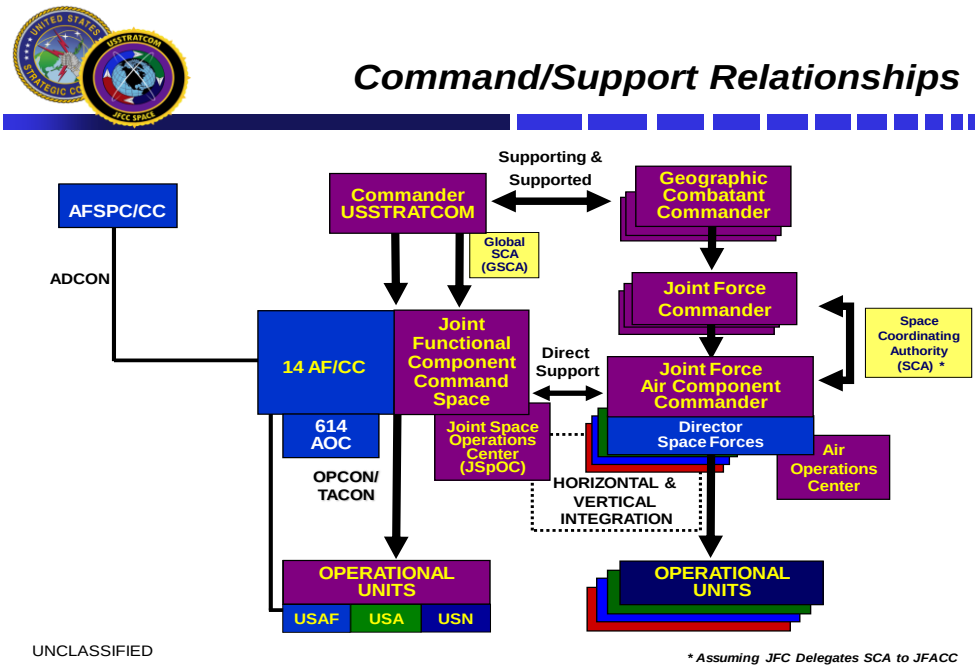

Figure 6: JFCC-Space Command and Support Relationships
Source: JFCC-Space Mission Brief, 18 Dec 2006

Figure 6 represents the command and support relationships of Air Force space forces. "The commander, JFCC Space (CDR JFCC Space), serves as USSTRATCOM's single point of contact for military space operational matters to plan, task, direct, and execute space operations. CDR JFCC Space will conduct space operational-level planning, integration, and coordination with other JFCCs, combatant commanders, other DOD, and non-DOD partners to ensure unity of effort in support of military operations, and national security operations. CDR JFCC Space will be the primary USSTRATCOM interface for operational space effects."[21] If the space forces deploy in-theater, the GCC will exercise COCOM and the service components will be delegated OPCON.[22] However, in some situations, it may be necessary to establish a direct support relationship

[21] AFDD 2-2, *Space Operations*, 10.
[22] AFDD 2-2, *Space Operations*, 13.

where the AOC can bypass the JSpOC and directly task a space unit for real-time information.[23]

The JFC commander must coordinate space power for the theater though their space coordinating authority (SCA), which "is an authority within a joint force aiding in the coordination of joint space operations and integration of space capabilities and effects. SCA is an authority, not a person."[24] "The JFACC is normally best suited to integrate space operations within a combined/joint force" and is normally delegated as the SCA for the JTF.[25] The JFACC brings the capability to command and control space forces through the AOC with reach back and direct liaison with the JSpOC. The JFACC also has the theater perspective necessary to ensure JTF strategic guidance and objectives are integrated into the overall space plan.

The JFACC, as the SCA, normally embeds a space operator into the ACCE to coordinate and integrate space capabilities and effects between the JFC and the components. The director of space forces (DIRSPACEFOR) serves as the senior space advisor to the JFACC.[26] The DIRSPACEFOR oversees many tasks for the JFACC including requirements deconfliction, prioritizing, and recommending space requirements; providing senior space perspective for strategy, operations, integration, and command and control of Air Force space forces.

Theater planning for space operations is conducted within the AOC in accordance with the joint operation planning process for air (JOPP-A) which results in a joint air and space operations plan (JAOP). The JAOP includes both request from global space support and tasking of theater space assets. The AOC embeds space expertise into the strategy, plans, and current operation divisions to ensure the ATO incorporates and synchronizes tasking of theater space forces.[27]

In concert with theater planning efforts, the CDR JFCC-Space plans global space effects through the joint space operations plan (JSOP). The JSpOC is responsible for command and control of global space operations and utilizes the same joint operation planning process for air to create the space tasking order (STO). The planners in the

[23] AFDD 2-2, *Space Operations*, 12.
[24] AFDD 2-2, *Space Operations*, 13.
[25] AFDD 2-2, *Space Operations*, 9.
[26] AFDD 2, *Operations and Organization*, 63.
[27] AFDD 2-2, *Space Operations*, 20.

JSpOC will prioritize and integrate requirements for global space forces from across multiple theaters of operation, maintenance of on-orbit assets, and then incorporate them into the space tasking order (STO). Following the same 72-hour planning cycle of the ATO, the global space planners must attempt to integrate all the theater requirements into one STO. This requires a high level of prioritization at the USSTRATCOM level to ensure as many space requirements are met as possible.

Space is integral to most modern military operations and space forces continuously provide services to the JTF (e.g. satellite communications, missile warning, PNT, and weather). However, at times special services are required to ensure mission effectiveness or to request effects more appropriate to space forces. For example, forces in Iraq and Afghanistan may request higher reliability from the Global Positioning Service (GPS) to ensure the most accurate service for precision guided weapons during a sensitive operation. The DIRSPACEFOR and assigned space operators in the AOC advocate and coordinate theater space requirements through the normal AOC planning processes.

During the TST process described above to demonstrate the command and control of airpower, space forces are also integral to the operation. The TST is using a RPV that is reliant on space for PNT and satellite communication services. To ensure the most accurate use of the precision guided munitions loaded on the RPV and minimize the chance of collateral damage, the DIRSPACEFOR and space operators embedded in the AOC COD requests support from the JSpOC to provide accuracy information of the GPS system prior to the strike. The JSpOC COD tasks the 2d Space Operations Squadron (2 SOPS) to analyze the GPS for optimal navigational accuracy for the geographical area and compares the data to the mission requirements. If required, the GPS can be enhanced temporarily or a recommendation to change the timing of the mission is forwarded back to the AOC. If necessary and feasible, balanced against other GCC requirements, the JSpOC will direct 2 SOPS to perform a temporary enhancement to the GPS before the strike.

This scenario demonstrates the need to centralize the control of the GPS system while maintaining responsive support to the theater. The unique attributes of the space domain include the environmental challenges of operating in space, the limited number of

assets available to support global operations, and the location of forces. For example, there are only about 30 GPS satellites on orbit at any one time, and they are not stationary above one point on the earth. The GPS satellites supporting the USCENTCOM AOR one minute will be supporting another theater, on the other side of the world, in six hours. The number and homogeneity of the force structure is much different also. There is only one squadron in the world responsible for the operation of the GPS constellation and it remains at home station to most effectively conduct operations.

Command and Control of Cyber Forces

Before 1991, Air Force Communications Command (AFCC) centralized the command and control of Air Force cyber forces. A local communications squadron provided services to the host wing, but was a tenant unit that reported to a geographically separated communications wing. In the early 1990s, the Air Force decided on a one base-one boss concept that restructured communications units; moving them under the direction of the host base wing commander and re-designated AFCC the Air Force Communications Agency (AFCA). This realignment of the communications squadrons ensured the priorities of the communications squadron were the same as the wing commander. Organizing, training, and equipping the communication unit were now the responsibility of the host wing.

When local area networks first began to proliferate in the Air Force, they were local solutions and designed, installed, and maintained by innovative airmen at the unit level. Soon, tactics, techniques, and procedures for squadron operations were developed that relied on these locally procured and administrated networks for mission success. Commanders became extremely reliant on "their network" to plan and implement Air Force operations, but the command and control of the network itself had no formal structure or design to ensure it was secure and resilient.

To combat this trend, the major commands (MAJCOM) created network operations and security centers (NOSC) to manage their command's data networks. The NOSCs attempted to professionalize the operation and management of the networks. They developed configuration procedures, improved network security, and enforced network standards. All bases within a MAJCOM were connected to the NOSC for services, security updates, and expert help desk support. However, there was no

overarching command and control system to integrate the networks. Between the MAJCOMs, situational awareness across the Air Force enterprise was difficult because each MAJCOM had different network equipment, standards, and configurations.

Contemporary air and space operations are extremely reliant on access to the cyberspace domain for operations and integration with the land and maritime domains. Cyber operations are inherently global in nature, conducted at near the speed of light, and require a cross-theater perspective to synchronize operations. To ensure air and space operations, it is necessary to plan for and include cyber operations in conjunction with planning air and space planning. As cyberspace grew in importance as a war-fighting domain, DOD recognized the requirement to command and control it in a systematic and purposeful way.

To achieve some level of control over cyberspace, the Unified Command Plan places responsibility for synchronizing the planning of military cyberspace operations under US Strategic Command (USSTRATCOM).[28] In June 2009, the Secretary of Defense (SecDef), Robert Gates, directed the Commander, US Strategic Command (CDRUSSTRATCOM) to "establish a subordinate unified command designated as US Cyber Command (USCYBERCOM)."[29] In addition, the SecDef directed CDRUSSTRATCOM to "disestablish the Joint Task Force – Global Network Operations (JTF-GNO) and Joint Functional Component Commander – Network Warfare (JFCC-NW) prior to full operating capability (FOC)" and for the services to identify "appropriate component support to USCYBERCOM to be in place and functioning prior to FOC." The Air Force subsequently established Twenty-fourth Air Force under Air Force Space Command (AFSPC) as the Air Force service component to USCYBERCOM, "aligning authorities and responsibilities to enable seamless cyberspace operations."[30] Although not at FOC at the time of this writing, Figure 7 displays DOD's proposed joint war-fighting relationships for the command and control of cyberspace.

These organizational changes demonstrate the importance of cyberspace to the defense of the nation. Removing the bifurcated management structure, assigning the

[28] Air Force Doctrine Document (AFDD) 3-12 (Draft), *Cyberspace Operations*, XX March 2010, 22.
[29] Honorable Robert M. Gates, Secretary of Defense, to Secretaries of the Military Departments, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, Commanders of the Combatant Commands, Assistant Secretaries of Defense, memorandum, 23 June 2009.
[30] Secretary and Chief of Staff of the Air Force to All Airmen, memorandum, 20 Aug 2009.

responsibility for command and control under one COCOM, and assigning service component commands provides unity of command and enhances unity of effort in cyberspace. Most importantly, the change clearly demonstrates that national leadership sees cyberspace as an operational war-fighting domain. To be most effective, doctrine is required to guide how the Air Force can best provide forces and integrate into the structure.

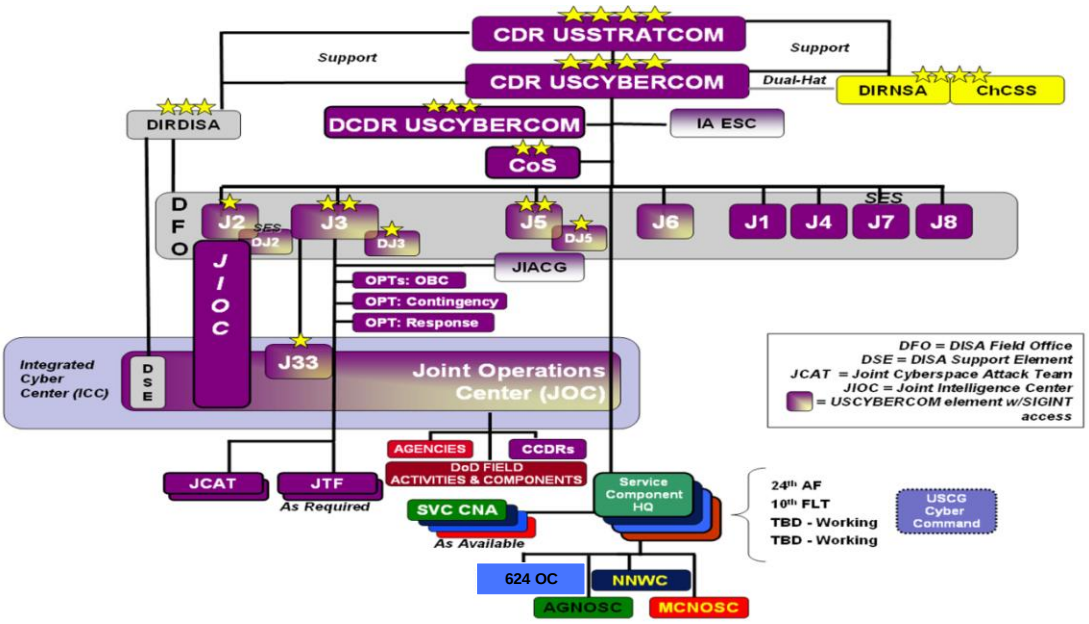

Figure 7: Cyberspace War-fighting Relationships
Source: *Enabling Concept for Command and Control of Cyberspace Forces*, 19 Jan 2010

The Enabling Concept for The Command and Control of Cyberspace is the Air Force's initial attempt to describe that "the Air Force cyber command and control mission is to establish, plan, direct, coordinate, and assess cyber operations in support of joint, service, and national interests."[31] The size and scope of Air Force operations make this job incredibly difficult.

To accomplish this, the Air Force assigned lead responsibility for organizing, training, and equipping the cyberspace forces to AFSPC. Under AFSPC, the Air Force created the Twenty-fourth Air Force and placed all major communications units under the

[31] Air Force Space Command (AFSPC), *Enabling Concept for Command and Control of Cyberspace Forces*, 19 Jan 2010, 6.

Twenty-fourth Air Force commander's direction. As the COMAFFOR for cyberspace, the Twenty-fourth Air Force commander exercises OPCON over assigned and attached cyber forces through the 624th Operations Center (624 OC). As the functional AOC for cyberspace, the 624 OC provides command and control of Air Force cyber forces through situational awareness and direction of all Air Force network operations to include computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE) through two integrated network operations and security centers (I-NOSC).

The communications squadrons and network control centers compose the overwhelming majority of forces and are responsible for computer network operations (CNO). CNO involves the installation and administration of the computer network hardware and software that form the backbone of the Air Force Information Network (AFIN). When executed, CNA is very centralized and strictly controlled; there are few units that perform this mission. CND is the responsibility of every airman at unit level to ensure proper measures are followed to limit the introduction of attacks. The 624 OC directs Air Force CND through the INOSCs and Network Control Centers (NCC). CNE is an intelligence function that takes advantage of adversary weaknesses to garner information through computer networks; it is also very centralized.

The Air Force soon consolidated MAJCOM NOSCs into two I-NOSCs that perform network operations and provide core services to the base communications units. The two I-NOSCs are responsible for centrally managing network services and security of the boundary protection devices. At the base level, the communications squadron's base network control centers (NCC) work for the wing commander; however, they are responsive to the I-NOSCs for operation of their segment of the AFIN. The NCCs provide on-site technical capability to implement physical and software network changes, modifications, and restoration when required.

To establish and operate network services in theater, the Air Force presents cyber forces to the GCC through the Air Expeditionary Task Force (AETF) construct. Combat communications units and base level communications squadrons forward deploy and are assigned to the theater under an expeditionary group or wing to provide base and wing

communications. These forces are OPCON to the theater COMAFFOR and provide the necessary network control center functions at the base level.

Twenty-fourth Air Force will establish an ACCE at USCYBERCOM to coordinate Air Force cyber operations with the objectives and intent of the combatant commanders. Because of the global nature of cyberspace, USCYBERCOM must synchronize cyber operations between all theaters simultaneously. Many of the same challenges the JSpOC experiences with respect to coordinating operations across multiple ATO cycles, apply to cyber operations requiring prioritization of theater effects by USSTRATCOM. To manage the global nature of cyberspace operations, the Air Force will deploy Cyber Operations Liaison Elements (COLE) with the theater AOC to coordinate requests for CNA from USCYBERCOM and Air Force cyber operations units.[32] "During routine operations, COLEs will work with the information operation teams, review standing OPLANs or CONPLANs from a cyber perspective; reaching back to the 624 OC for assistance with developing mission assurance plans for the supported AOR. For crisis/contingency operations, COLEs will receive real-time reach back support for all cyber capabilities from the 624 OC."[33]

The 624 OC command and controls cyber forces and directs execution by utilizing the joint operation planning process for air to create the cyber equivalent of the JAOP, the Cyber Operations Directive (CyOD) and associated orders. The CyOD provides the overarching strategic level guidance used to develop the Air Force cyber tasking order (AF-CTO). The purpose of the AF-CTO is to employ capabilities and direct Air Force "cyber assets and organizations in support of USCYBERCOM and combatant commander needs."[34] Twenty-fourth Air Force uses the cyber control order (CCO) "to actually build and shape the portion of cyberspace to be employed in support of combatant commander objectives."[35] Finally, the maintenance tasking order (MTO) directs infrastructure changes, upgrades, maintenance, and patch management to the AFIN. In a Directive memorandum to the MAJCOM commanders, the Air Force Chief of Staff clarified the authority of the Air Force Network Operations Commander by

[32] AFSPC, *Enabling Concept for Command and Control of Cyberspace Forces*, 5.
[33] AFSPC, *Enabling Concept for Command and Control of Cyberspace Forces*, 15.
[34] AFSPC, *Enabling Concept for Command and Control of Cyberspace Forces*, 7.
[35] AFSPC, *Enabling Concept for Command and Control of Cyberspace Forces*, 7.

stating these orders "are military orders issued in the name of the Air Force Chief of Staff and by order of the Secretary of the Air Force."[36]

The enabling concept for command and control of cyberspace demonstrates cyberspace support to a theater operation will follow the same mission thread of a TST using a weaponized RPV. A cyber support or mission request from a theater GCC is forwarded to and approved by USSTRATCOM (through USCYBERCOM) for COMAFFOR-Cyber to provide mission assurance support to a TST operation. Direct liaison authority (DIRLAUTH) is granted between the 624 OC and the theater AOC to coordinate and prepare a mission assurance operation to support the strike.[37] The embedded cyber expertise in the theater AOC and the COLE begin reach-back operations to the 624 OC to leverage air component cyber operation and planning capabilities.

The 624 OC will direct the I-NOSC supporting the theater to initiate a risk assessment for the strike by analyzing the circuits supporting theater RPV operations. The 624 OC executes "instantaneous TACON" of the NCCs supporting the operation and surges cyberspace forces for the highest level of mission assurance.[38] The 624 OC must also coordinate with interagency partners such as the Defense Information Systems Agency (DISA) for those services and circuits provisioned outside Air Force control. If necessary, the 624 OC adjusts the network defense posture to reflect the increased threat or the need for increased network security during the strike. Once the theater commander or designee makes the engagement decision and approves the strike, the 624 OC monitors the operation and takes necessary actions until the mission is complete.

One Air Force, One Command and Control Approach?

The command and control approach for air power has maturated from a century of experiments and trials in conflict to suggest that centralized control and decentralized execution is the best way to realize unity of effort and flexibility. The Air Force fought to ensure air power was controlled by a single airman, eventually resulting in the creation of the JFACC. Although doctrinally space forces also follow the tenet centralized control and decentralized execution, there is not much evidence of decentralized execution

[36] Gen Norton A. Schwartz, Chief of Staff, US Air Force, to ALMAJCOM-FOA-DRU/CC, memorandum, 15 May 2009.
[37] AFSPC, *Enabling Concept for Command and Control of Cyberspace Forces*, 14.
[38] AFSPC, *Enabling Concept for Command and Control of Cyberspace Forces*, 16.

because the global nature of the domain and the limited number of assets. It now appears that the Air Force is borrowing heavily from the design of the space command and control structure due to the global nature of cyberspace.

The seventeen air and space functions vary in the domains utilized, number of forces available and the range and speed at which they operate. The unique environmental attributes of the domain, the character of conflict, and the force structure influence the command and control approach within each domain. Because the Air Force can lay claim to having the preponderance of force, expertise, and the ability to command and control in the air and space domains, the JFACC normally also serves as the JTF's SCA. The Air Force does not have one approach to command and control for all three war-fighting domains.

With the exception of intra-theater airlift and some strategic bombers, command and control of airpower is designed for theater operations and theater air operations still require a high level of centralized control to deconflict and coordinate effects. The JFACC attempts to adhere closely to the preferred method of centralized control and decentralized execution during high-tempo combat operations and when required, transition to a highly centralized process to manage strategic imperatives and direct the most restrictive conditions, such as in the execution of some TSTs.

The TST process demonstrates how the synchronized effects of air, space, and cyberspace play a vital role in one operational thread. The TST scenario also shows how even in the air domain, there is a tendency to centralize command and control if the technology is available to do so, if operations require the rapid synchronization of several types of forces, and if the impact is potentially strategic. However, even a sensitive operation such as a TST can be over centralized and limit airpower's flexibility. A different approach could be to lower the decision authority with proper ROEs which could be more effective and resilient during a multiple TST scenario.[39]

Unlike in the air and space domains however, the Air Force typically does not have the preponderance of the cyber forces in a JTF. Although all three domains overlap and intersect, and all three domains attempt to follow the joint operations planning process for air as a planning framework, they diverge from doctrine where appropriate.

[39] Kometer, *Command in Air War*, 285.

The space domain is a global force and faces significant challenges attempting to synchronize space effects for all theaters simultaneously. The Air Force has created the DIRSPACEFOR in the AOC as the JFACC's space expert to coordinate space support for the JTF. Deploying space expertise throughout the AOC helps ensure the theater utilizes space smartly. Since space assets are limited, the Air Force can command and control utilizing this arrangement. As the GPS example shows, most times there is only one subordinate space unit that performs a specific mission, which creates a centralized, but very flat organization.

The maturation of networks in the Air Force tracked the importance of cyberspace to the global community. The centralization of management of these networks provided shared services, standardization, and expertise that the bases did not have inherent to the wing. However, even as MAJCOM NOSCs consolidated and managed computer networks, the ability to tailor services to diverse requirements remained decentralized. The Air Force way ahead is to implement a centralized command and control approach that will attempt to impose order over the domain.

AFSPC has created an initial command and control structure for cyberspace forces with Twenty-fourth Air Force and the 624 OC as the lead elements. A bifurcated command and control structure for computer network operations and CNA is created by aligning the communications squadrons responsible for the installation and operation of local portions of the network under wing and base commanders while Twenty-fourth Air Force controls the CNA mission. By assigning a cyber specialist in the form of a COLE to coordinate reach back support with the 624 OC, the new concept for command and control of cyberspace is very similar to the DIRSPACEFOR approach for space forces. However, the unique attributes of the environment, forces, and the character of conflict in cyberspace should determine the best command and control approach. The next chapter examines the character of each domain and proposes a cyberspace command and control approach.

Chapter 3

A Cyberspace Command and Control Approach

Confronted with a task, and having less information available than is needed to perform that task, an organization may react in either of two ways. One is to increase its information processing capacity, the other to design the organization, and indeed the task itself, in such a way as to enable it to operate on the basis of less information. These approaches are exhaustive; no others are conceivable. A failure to adopt one or the other will automatically result in a drop in the level of performance.

— Martin van Creveld

A prince or general can best demonstrate his genius by managing a campaign exactly to suit his objectives and his resources, doing neither too much nor too little.

— Carl von Clausewitz

The proliferation of command and control systems throughout the Air Force has provided commanders with an abundance of information to process. Although communication technology and information processing power rapidly advanced during the past half century, the process by which decisions are made has changed little. Hierarchical Napoleonic staffs still are prevalent, but are now confronted with far greater amounts of information to process, orient, and decide upon, leaving only the act (and sometimes not that portion) to subordinate units. The Air Force must create a structure and develop a command and control approach that protects the air, space, and cyberspace domains and assures the operations conducted in and through each of them.

While every war-fighting domain is subject to the laws of physics that govern their physical environment, the rate of change and speed of access to cyberspace results in almost incalculable complexity. The cyberspace organizational structure and command and control approach must be as agile and responsive as the systems and personnel it is intended to control. Important differences in the domains define the problem space and should influence the organizational structure and command philosophy where "the strategist must concentrate less on determining specific actions to be taken and far more on manipulating the structure within which all actions are determined."[1]

[1] Everett C. Dolman, *Pure Strategy: Power and principle in the space and information age* (New York, NY: FRANK CASS, 2005), 4.

	Air	Space	Cyberspace
Operating Environment	Theater Specific	Global	Very local to Global
Access	Limited - Can be denied	Very restricted - Only a few - Easy to deny	Very open - Everyone - Difficult to deny
Pace of Ops	Very high to low	Moderate (constant)	Very high
Forces	Low density - high demand Very diverse Joint ops/coalition	Very low density - high demand Not very diverse	Large "every airman" High demand Spans all domains
Level of Training	Very high	High	Varies widely
Net centricity / Connectivity	High /various	Very high	Complete connectivity
C2 Approach	Centralized Control & Decentralized Execution	Centralized Control & Centralized Execution	Centralized Control & Decentralized Execution

Figure 8: Domain Characteristics
Source: Author's original work

Different Domain Characteristics

Figure 8 depicts a comparison of the environmental and operational characteristics of each domain. Centralized control of theater air power under the command of an airman is a key tenet of air and space power. The characteristics of the air domain are well suited to this type of control approach to ensure limited theater air assets are most efficiently utilized and effectively deconflicted. The AOC is generally concerned about a specific theater area of operations with definable borders. The Air Force can normally achieve a level of air superiority over this area; limiting what friendly assets are in the airspace and effectively defending that airspace from enemy air power. The pace of operations in the air can vary widely from a high tempo during the first phases of a conventional conflict to relatively low levels in support of peacekeeping operations. The AOC has procedures and a flexible command structure to allow lower echelons to decentralize execution according to rules of engagement when possible, but is prepared to centralize control of execution when necessary. Air forces are highly specialized and require several operational specialties to perform diverse missions

ranging from strategic bombing to tactical airlift. Each mission area requires highly trained and specialized forces to execute. This specialization requires an extraordinarily high level of training to be effective in the air domain. Once trained, aircrews are specialist in a specific weapon system and held accountable for their actions. Finally, the network centricity, connectivity and information sharing, within the domain is high but gaps and stovepipes remain.

Although space operations doctrinally follow the tenet of air and space power, centralized control and decentralized execution, in actual practice the space domain is command and controlled with a centralized control and relatively high level of centralized execution. Centralization works well for a force that must coordinate the use of extremely limited assets across multiple theater commanders daily. Access to space is very limited, only a few countries in the world have the capability to operate effectively in space on their own. To date, only the US, Russia, and China have demonstrated an operational anti-space capability, and are the only countries that currently could practice any serious level of space control.[2] The pace of global space operations is relatively constant because the JSpOC is responsible for operation and maintenance of space assets regardless of a theater's pace of operations. The forces that command and control space operations and keep space assets on orbit are specialized and well trained. However, space operators can move from one weapon system to another with relative ease compared to the specialization required of aircrews. Because of the wide range in age of active space systems, the level of connectivity and network centricity can vary widely.

The characteristics of the cyberspace domain are quite different from the air and space domains. The Air Force is attempting to centralize the command and control of the domain to one numbered air force responsible for all Air Force networks. However, the large force structure and dynamic operating environment will make it very difficult to gain control over the domain. The pace of operations in cyberspace is at nearly the speed

[2] An excellent description of the newest entrant, China, and the Chinese ASAT capability is presented by Ian Easton, *The Great Game in Space: China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy* (Arlington, VA: The Project 2049 Institute), available online at http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf (accessed 25 April 2010).

of light requiring "extremely short decision-making cycles."[3] Cyberspace forces are the most diverse of the three Air Force domains; the user on a terminal in the security forces squadron and the network attack expert in 24th Air Force are both *operating* in cyberspace.[4] Cyberspace provides global connectivity, but in general, each element performs a local service. The Air Force identified previous training of cyberspace operators as being not sufficient or consistent; a difficult problem to address in a domain where the weapon systems are on a three to five year life cycle. Network centricity in cyberspace is almost complete where, within the limits of security, most systems are either already connected or able to be connected. The attributes of cyberspace open a range of command and control approach possibilities the Air Force can pursue.

The air, space, and cyberspace domains currently employ what the authors of *Power to the Edge* would describe as Industrial Age command and control approaches.[5] While an Industrial Age approach can vary according to the environment, communications capabilities, volume of information, professional competence, and the initiative of subordinate commanders, it implies a level of centralized control based on orders from the operational level.[6] The approaches for air and space have proven to be highly effective and capable of sufficiently responding to a wide range of operational tempos. However, the cyberspace domain has yet to be challenged by a significant competitor during a major conflict.

The placement of the cyberspace mission under AFSPC provides the necessary oversight of a MAJCOM with relevant operational expertise and knowledge of communications technology. However, while space and cyberspace are extremely reliant on each other for operations, the difference between the domains is stark. The different composition of forces, ease of access to the domain, and pace of operations can seriously affect the ability to centralize both command and control and execution with great affect in the cyberspace domain. Also, with every theater involved in cyberspace operations simultaneously, problems with span of control and information overload will quickly

---

[3] Department of Defense, *The National Military Strategy for Cyberspace Operations, December 2006* (Washington DC: Department of Defense, 2006), 11. Document is now declassified.
[4] Maj Gen Webber, interview by author, 22 March 2010.
[5] David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington DC: DoD Command and Control Research Program, 2003), 18.
[6] Alberts and Hayes, *Power to the Edge*, 19.

emerge. History has shown in the air domain that "the more a decision maker tried to use near-complete information to manage the details of subordinate actions, the less they were able to handle the inevitable uncertainty that accompanied war—the less they were able to act like a "learning organization."[7] The requirement to respond rapidly to change requires a different approach.

Cyberspace: A Domain of Warfare

To reduce costs, the Air Force has historically applied a civilian management philosophy to the command and control of cyberspace. The move to homogeneous operating systems, support software, and hardware has been very cost effective by simplifying network management, reducing training requirements, and improving network change management. Homogeneity of network infrastructure also increases the capability to provide situational awareness to higher echelons, which is necessary to effectively command and control the domain. In response to the various service, contractor, and industry networks supporting the joint environment, *The United States Air Force Blueprint for Cyberspace* claims, "it is both necessary and inevitable to integrate and synchronize these networks while transitioning to a single seamless network."[8] The current architecture and enabling concept may work well during relatively low levels of conflict against less technically competent competitors. However, movement to a centralized homogeneous architecture will also introduce unintended risks to operations.

If cyberspace is a domain of warfare, then it is subject to war's nature and the friction, both chance and uncertainty, that Carl von Clausewitz described as being prevalent in war, where "everything is very simple, but the simplest thing is difficult. The difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war."[9] Friction can take the form of political restrictions on the use of cyberpower, new actors entering the battlespace, and attacks being difficult to detect and attribute. Chance can come from multiple sources, internal errors or opportunities, environmental impacts and disasters, and external influences upon the

[7] Michael W. Kometer, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower* (Maxwell Air Force Base, AL: Air University Press, 2007), 270.
[8] Air Force Space Command (AFSPC), *The United States Blueprint for Cyberspace*, 2 November 2009, 4.
[9] Carl Von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 119.

system. Uncertainty is prevalent in cyberspace where it is very difficult to identify an "act of war" or attribute the attacks to a specific group or nation state. Technology provides new methods and forms of personal interaction in cyberspace that soon become a necessity for mission success. The projections of the advancements in technology are consistently inaccurate where new technology is constantly being created and old technology becomes obsolete. These difficulties combine to make the cyberspace domain especially difficult to conform to any definition of control.

While the enduring nature of warfare may be prevalent in cyberspace, the character of cyberwarfare is distinct from other domains. To be successful, an agile command and control approach is necessary in the information age. As professed by Arquilla and Ronfeldt in *Cyberwar is Coming!*, "waging cyberwar may require major innovations in organizational design, in particular a shift from hierarchies to networks. The traditional reliance on hierarchical designs may have to be adapted to network-oriented models to allow greater flexibility, lateral connectivity, and teamwork across institutional boundaries."[10]

Agile Command and Control in Information Age Warfare

It is important to understand the cyberspace is a war-fighting domain. This mandates the creation of organizations to advocate for resources, develop programs, and provide trained and equipped forces to deliver cyberspace capabilities for the Air Force. The way the Air Force approaches command and control in the domain must be determined by the command and control problem space and where it fits into the command and control approach space.

The authors of *Understanding Command and Control* propose the command and control problem space represented in Figure 9, which depicts how the three dimensions of strength of information position, rate of change, and familiarity define the type of problems an organization faces and where they will reside in the problem space.[11] A classic hierarchical organization would reside in the lower left, front corner of the cube.

[10] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" in *In Athena's Camp: Preparing for Conflicts in the Information Age*, ed. John Arquilla and David Ronfeldt (Washington DC: RAND, 1997), 45.
[11] David S. Alberts and Richard E. Hayes, *Understanding Command and Control* (Washington DC: DoD Command and Control Research Program, 2006), 75.

An extreme example of this type of problem is a highly controlled activity such as nuclear missile operations. Centralization of nuclear weapons and space systems is highly desired because the cost of failure or a misstep is too costly. The primary objective in the nuclear command and control domain is to follow directions to the letter when ordered, not to adapt to changing conditions through innovation.

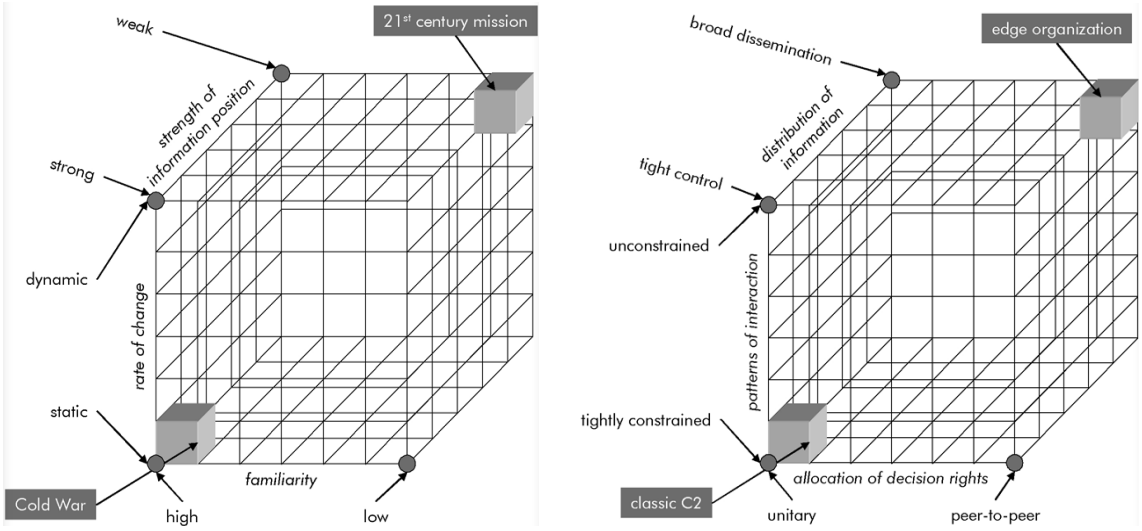

Figure 9: Command and Control Approach Space and Problem Space
Source: DoD Command and Control Research Program, *Understanding Command and Control*

At the other end of the spectrum is where the information age mission problem space resides. This problem space has a weak information position, a high rate of change, and familiarity with the problem is low. To cope in this environment militaries will need to adopt "better mechanisms for sharing information and collaboration, more knowledgeable personnel, and better trained personnel" and "a different command and control approach."[12]

The mission, or problem space, largely determines where in the approach space cube an organization should reside. Represented in Figure 9, the approach space is defined by the allocation of decision rights, patterns of interaction, and distribution of information. The problem space to which an organization must adapt significantly

[12] Alberts and Hayes, *Understanding Command and Control*, 86.

affects where in the command and control approach space they will reside. An organization is not necessarily in a single position; rather, they change their approach according to the mission.[13]

The most restrictive approach, the classic command and control approach, severely restricts interaction, distribution of information, and centrally controls decision rights. At the other extreme is what the authors would describe as an edge organization. Edge organizations have greatly enhanced peer-to-peer interactions, limit middle management, and concentrate on creating initial conditions that will make success more likely for rapidly changing conditions.[14] An edge organization resides in an approach space that allows complete allocation of decision rights, unconstrained interaction between entities, and broad distribution of information necessary to make decisions.

The challenge is to determine where in the approach space cube a military organization should place themselves for maximum combat capability. There is a danger of planning and structuring the command and control for cyberspace only to be flexible enough to work one type of problem; synchronous, low-level, and single theater operations. The cyberspace approach should be exceptionally agile to effectively deal with the dynamic character of warfare in the domain. The domain is at the heart of enabling information age warfare and the Air Force must be as close to an edge organization as possible while still being able to provide some level of control. The operating environment will place increased stress on commanders as they are faced with unfamiliar scenarios in complex, uncertain, and rapidly changing situations.

The authors of *Power to the Edge* postulate that there are six aspects of agility an agile command and control organization requires:[15]

- **Flexibility** – the ability to employ multiple ways to succeed and the capacity to move seamlessly between them
- **Innovation** – the ability to do new things and the ability to do old things in new ways
- **Adaptation** – the ability to change work processes and the ability to change the organization
- **Resilience –** the ability to recover from or adjust to misfortune, damage, or a destabilizing perturbation in the environment

[13] Alberts and Hayes, *Understanding Command and Control*, 76.
[14] Alberts and Hayes, *Power to the Edge*, 5.
[15] Alberts and Hayes, *Power to the Edge*, 128.

- **Robustness –** the ability to maintain effectiveness across a range of tasks, situations, and conditions
- **Responsiveness –** the ability to react to a change in the environment in a timely manner.

Comparing the current cyberspace command and control approach to the six requirements for agility reveals some possible issues. First, flexibility is used here in reference to the cognitive domain, where a highly centralized system may retard the generation of ideas if completely reliant on the central controlling entity. Centralization may be effective when expertise is required to rapidly formulate a solution to a technical problem. However, the Air Force is very diverse and joint and coalition partners add more complexity. In addition, cyberspace operations must be rapidly coordinated down to the lowest-level echelons to ensure actions are complete and effective.

Innovation has been the hallmark of progress in cyberspace, both in the advanced technology that provides more, better, faster, and richer information services and the new ways individuals communicate and build work processes. Centralizing cyberspace expertise and approval for new systems at Twenty-fourth Air Force will likely provide a more secure environment. However, if significant resources are not dedicated to the development and approval of new systems, innovation will be much more arduous and slow.

Adaptation is the ability to alter the organization and work processes as necessary and is a strength of the new cyberspace command and control structure. If most cyberspace organizations are under the command of Twenty-fourth Air Force, they will be able to make changes as necessary without coordination and agreement with multiple outside organizations.

Resilience to attacks or friction is necessary to achieve mission assurance of Air Force operations. There are multiple ways to enhance resilience to cyberspace operations both organizationally and technically. The Air Force has a very resilient network architecture with redundant and backup systems; however, in addition to the technical structure, the Air Force could attain further resilience by dispersing decision making to improve the quality of the decisions and reduce disruptions due to the loss of the centralized operations center.

The wide variety of operations performed and units supported make the aspect of robustness very important to cyberspace. It is true that there are many redundant, stovepipe systems on the network whose requirements could easily be incorporated by existing services to reduce costs, increase simplicity, and provide better support. However, sometimes standardization is at the expense of optimization of mission systems that are specialized to support specific mission areas.

Responsiveness in a centralized command and control approach can have its benefits and drawbacks. With the proper situational awareness, the ability to react rapidly to changing conditions can be a positive attribute of Twenty-fourth Air Force's centralized control and execution approach since they will be able to determine a course of action and implement it rapidly across the domain. *The United States Air Force Blueprint for Cyberspace* calls for a focus on "mission assurance" to be able to survive attacks on Air Force systems and "retain the ability to respond-thus giving us mission assurance in the face of future attacks or other disruptions."[16] However, if lower echelon cyber operations units had the situational awareness and capacity for sense making that a network centric environment can provide, they may be able self-synchronize and begin to take responsive actions based on pre-existing rules of engagement.[17]

While analyzing the history of command and control, Martin Van Creveld recognized similar issues that the Air Force is currently struggling with in the cyberspace domain. He writes, "Returning now to the two basic ways of coping with uncertainty, centralization and decentralization, it must be noted that they are not so much opposed to each other as perversely interlocking. In war, given any one state of technological development, to raise decision thresholds and reduce the initiative and self-containment of subordinate units is to limit the latter's ability to cope on their own and thus increase the immediate risk with which they are faced; in other words, greater certainty at the top (more reserves, superior control) is only bought at the expense of less certainty at the bottom."[18] War is a complex and chaotic activity; it cannot be controlled in a precise, predictable way. Cyberspace is subject to the same challenges of the other war-fighting domains where command and control approaches that attempt to achieve perfect

[16] Air Force Space Command (AFSPC), *The United States Blueprint for Cyberspace*, 2 November 2009, 4.
[17] Alberts and Hayes, *Power to the Edge*, 140.
[18] Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 274.

situational awareness and centralized control will fail in the face of an active thinking enemy.

A Hybrid-Network Approach

It is imperative to create a structure to control centrally when required, yet provide the freedom and ability to survive operational shock, perturbations in the system and lower echelons to operate without direction or support from the central entity when necessary. To achieve this flexibility, a hybrid command-network approach will prove most promising for cyberspace. This structure, recommended by David Lonsdale, in general reference to war-fighting organizations, can be very effective in the cyberspace domain.[19] The hybrid-network retains the hierarchical organizational structure the Air Force is accustomed to operating with while permitting the "free flow of information horizontally, vertically, or allowing the information to jump echelons as necessary for mission accomplishment.[20] A possible form of this structure is depicted in Figure 10. It can vary its approach according to the different problem spaces of network operations, defense, attack, or exploitation; retaining some form of centralization where necessary and decentralization when appropriate. The necessity to achieve a level of situational awareness that allows the organization to ensure operations are conducted under the COMAFFOR-Cyber commander's intent, the ability to use the "directed telescope" where necessary, to provide upper echelon expertise when requested, and for lower echelons to retain the capability to function when disconnected.

There are many benefits to the dispersion of expertise and decision authorities. As van Creveld cautions, "exercising central control over limited resources is one way of maximizing cost-effectiveness, distributing those resources among subordinate units may, by virtue of eliminating much of the need for planning, coordination, and internal communication, be another. Since disruptions in the communications process and consequently uncertainty, are inherent in war, I would suggest that distributing the resources may often be the more effective way to maximize cost effectiveness."[21] In addition, the cyberspace units operating the network at the base level NCC must be able

[19] David Lonsdale, *The Nature of Warfare in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 125.
[20] Lonsdale, *Nature of Warfare in the Information Age*, 125.
[21] Creveld, *Command in War*, 271.

to be as flexible as the requirements of the units they are supporting. As network centric operations pervade the force, the NCC must retain the capabilities to respond rapidly to local requirements.

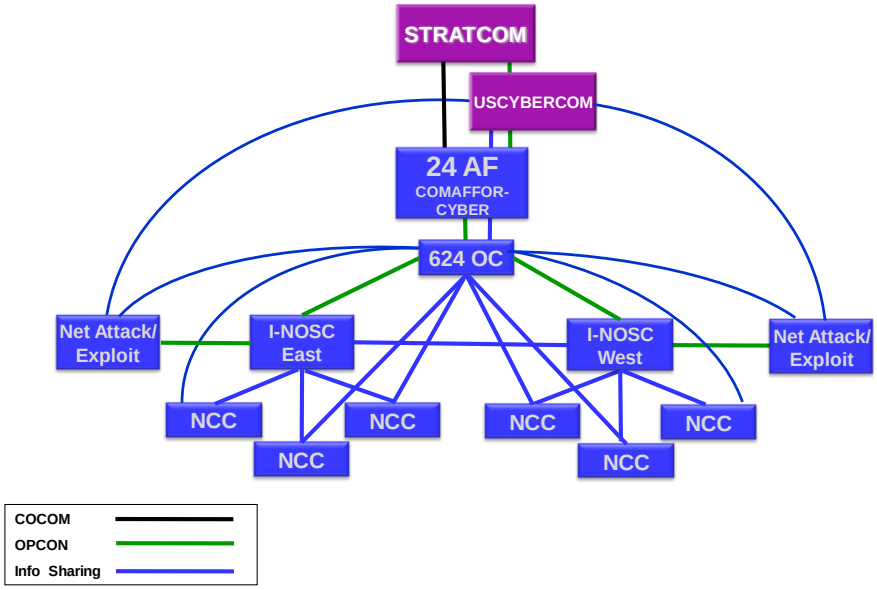

Figure 10: Hybrid Network Command and Control Approach for Cyberspace
Source: Author's original work

Situational awareness of Air Force cyberspace is certainly not where it could and should be with the technology available today. However, to believe that technology can make warfare less complex by providing perfect information belies the fact there is an enemy on the other side countering and planning to defeat the next move. Clausewitz describes the aim of warfare as being "to disarm the enemy" and it cannot be accomplished according to a scripted plan due to the interaction of forces where "he dictates to me as much as I dictate to him."[22] To program the war and preplan every action in advance to ensure victory is to posture the force for significant setbacks and possible defeat. The 624 OC must have visibility into what the CNA units, NCCs, and I-NOSCs are doing, but refrain from conducting tactical operations. If they concentrate on the tactical details, they will do so at the expense of the operational and strategic focus.

[22] Clausewitz, *On War*, 77.

In addition, concentrating the expertise at the 624 OC can create a single point of failure and place Air Force networks at a higher risk to system perturbations if capabilities are not adequately dispersed. A command and control approach that provides lower echelons direction on what to accomplish, yet leaves some capabilities to do so is more robust and survivable.

An unexpected form of attack can completely compress the decision cycle to defend the network. A reactive approach to network defense does not allow for a rapid process across the AFIN. With only minutes or hours to determine an effective course of action, rapid response may require operators to pre-program some actions in cyberspace. However, the enemy does not have to act according to plan and once they observe an automated response, they can change their method of attack or defense posture to parry the next strike. The proposed hybrid-network is a more proactive and survivable approach that can better support mission assurance.

The growth of cyberspace in the Air Force resembles the development of a complex, self-organizing, adaptive system. The decisions made today about the best command and control approach for cyberspace will determine how the Air Force is postured to survive, respond, and assure operations in the air and space domain in tomorrow's conflict. Although the hybrid network is not infallible, its span of control attempts to address the challenge that no one entity can command cyberspace using a hierarchical-centralized organization. "So long as command systems remain imperfect—and imperfect they must remain until there is nothing left to command—both ways of coping with uncertainty will remain open to commanders at all levels. If twenty-five centuries of historical experience are any guide, the second way will be superior to the first."[23] Cyberspace forces and the war-fighting network must be command and controlled with elements of both a hierarchical and network approach. An agile command and control approach can better transition from low-level conflicts to a high-level conflict against a near peer adversary. Cyber warfare at near the speed of light will demand this agility.

[23] Creveld, *Command in War*, 274.

Conclusion and Recommendations

Confronted with a task, and having less information available than is needed to perform that task, an organization may react in either of two ways. One is to increase its information processing capacity, the other to design the organization, and indeed the task itself, in such a way as to enable it to operate on the basis of less information. These approaches are exhaustive; no others are conceivable. A failure to adopt one or the other will automatically result in a drop in the level of performance.

— Martin van Creveld

A prince or general can best demonstrate his genius by managing a campaign exactly to suit his objectives and his resources, doing neither too much nor too little.

— Carl von Clausewitz

The Air Force's most effective approach to command and control of cyberspace must be as agile as the network centric operations it is designed to support. Above all, it is crucial that the Air Force command and control cyberspace with a philosophy of enabling and enhancing operations in the air and space domains to ensure success on the ground. Cyberpower is now a significant national capability and the United State's ability to protect and operate will be contested during the next major conflict with a near-peer competitor. The Russians successfully demonstrated how a nation might attack another's cyberspace capabilities in the initial stages of conflict to create confusion during their offensive on Georgia. The US Air Force's military dominance is heavily reliant on its technological advantage and cyberspace superiority and can expect opponents to attack it early and often.

Cyberspace has joined the other war-fighting domains as critical to the security and economic well-being of both nation-states and multinational groups in the 21st Century. Eventually, the land, sea, and air domains each had theorists propose how the respective domains were critical to national prosperity and survival. The theories proposed by Julian Corbett and Alfred Mahan for the sea, or Giulio Douhet for the air domain, influenced how the nation and the respective services were organized and

equipped.[1] Without the benefit of a theory of cyberspace warfare, the Air Force is currently leading the DOD to establish doctrine that could help "warn us the moment we begin to leave the beaten track, and enable us to decide with open eyes whether the divergence is necessary or justifiable."[2] However, theory and doctrine are difficult to create without a broad range of experience. The task is more difficult because simply defining cyberspace involves all the other domains since it is largely a manufactured domain and made more challenging because the entire domain is replaced every three to five years through the advancement of technology. No other domain faces such dynamic change and speed of operations as cyberspace.

The architecture of cyberspace makes it extremely challenging to confront the myriad of competitors in the domain. Attempts to achieve cyberspace superiority will not be complete; rather, as Corbett defined sea control, the best one can hope to achieve is at a specific place and time.[3] Corbett defines sea control as "control of communications, and not, as in land warfare, the conquest of territory."[4] His theory is similar in another respect with cyberspace where the point of sea control is to support the army on land; the central point of cyberspace control is to enable operations in the other war-fighting domains.

Although cyberspace is a relatively new domain, command and control is as old as warfare. The advancement of communications technology and command and control has been inextricably linked since the first telegraph was used. Napoleon had little technology to assist him control vast armies across great distances, his genius was at the center of a centralized command structure, supported by a staff system that provided filtered reports from subordinate echelons to guide his directed telescope where and when needed.

To account for the lack of genius, the Prussians created a professional, educated staff that would systematically plan and control forces. The benefits of the telegraph to planning large operations and to controlling the deployment of forces moved Moltke to

---

[1] C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven: Yale University Press, 1990), 244.
[2] Julian S. Corbett, *Some Principles of Maritime Strategy* (Annapolis, MD: Naval Institute Press, 1988), 10.
[3] Corbett, *Some Principles of Maritime Strategy*, 91.
[4] Corbett, *Some Principles of Maritime Strategy*, 94.

direct its installation at the first opportunity to achieve unity of effort and provide situational awareness. Similar to the ubiquity of network communications technology today, although the telegraph was a great leap forward in communications, the enemy had access to the same technology as the Prussians and the telegraph was subject to the friction of war where interruptions, lack of mobility and the enemy immediately began to attack telegraph lines to disrupt communications. To account for this friction, the Prussians employed the operational philosophy *Auftragstaktik* to ensure that when necessary lower-echelon headquarters would act under the general guidance of the commander's intent.

World War I saw many technological advances in weapons and communications. In order to cope with vast armies employing terrific firepower, headquarters staffs attempted centralized control of operations via the telephone; and it failed miserably. The telephone was unable to control mobile offensive operations. In contrast, fixed position, defensive operations could take advantage of the telephone's capability to achieve unity of effort and to concentrate firepower.

Both centralized and decentralized approaches to command and control were effective when employed under circumstances that favored their strengths and accounted for their weaknesses. The German *blitzkrieg* tactics of World War II demonstrated a drastic increase in mobility enhanced by improved wireless communication and a decentralized command and control approach, which quickly defeated the defensive tactics of World War I. In contrast, by combining radar, telephone and radio communications, and a centralized command structure, the British centralized the defense of the home island to achieve unity of effort to defeat the Germans in the Battle of Britain.

Soon missile, satellite, and computer technology combined to provide a previously unimaginable view of the battlefield and the ability to communicate globally. Vietnam saw the first satellite communications between the national leadership and the commander in theater. However, the failures of missions in Iran and inter-service communications challenges of Granada moved the DOD to establish joint organizations with a single joint force commander and component commanders to direct operations in each domain. The Gulf War demonstrated the first use of a JFACC as the single airman

responsible for all airpower in the theater of operations. The AOC, tactical data links, and computer networks connected forces from the national command authority to the front lines. The United States dominated the use of the technology in the information age and the world took notice.

Network centric warfare was proposed as a new doctrine for how militaries in the highly connected information age must interact and rapidly respond to changing conditions. With military forces heavily reliant on data networks, access and denial to information and the electro-magnetic spectrum gained importance as a form of warfare. Out of Myer's Signal Corps, airpower grew rapidly into a war-fighting domain, now cyberpower, in its own right, has grown into new domain of warfare. The command and control of that new domain presents new challenges for the Air Force.

The tenet of centralized-control and decentralized execution has proven to be flexible enough to account for multiple levels of conflict. As a matter of doctrine, the Air Force decentralizes execution in the air domain, but when necessary, can centralize decision authority. Similarly, space support has become pervasive throughout most military operations. Global operations and limited assets make it imperative to plan and apportion centrally while attempting to meet multiple GCC requirements through the JSpOC. However, contemporary command and control approaches in the air and space domain reflect the inherent attributes of the environment within which they operate.

The Air Force must not attempt to apply the space command and control template to cyberspace; rather it must establish the doctrine and organizations most appropriate to address its unique challenges. The stand-up of Twenty-fourth Air Force to plan and conduct cyberspace operations as the Air Force component to USCYBERCOM is a significant first step in integrating cyberspace operations with the air and space domains. The deployment of COLE's is an attempt to incorporate and synchronize cyberspace operations into air and space operations through the theater AOC. This integration is essential to an operation like a TST, where the air, space, and cyberspace domains are inextricably linked to execute most operations in the contemporary battlespace.

The TST also demonstrates how flexibility in command and control approaches is imperative; to decentralize when possible and to centralize when necessary. However, the TST example is a simplified single event, conducted with available assets during a

low-level conflict. The current cyberspace enabling concept reflects a well-thought out plan to command and control cyberspace forces under the current structure and battle rhythm. However, a conflict with a near-peer competitor, under high ops tempo may not allow a central node to effectively address and respond to all the GCCs theater requirements. To reduce costs, the Air Force has adopted a civilian management philosophy to the command and control of cyberspace. The move to homogeneous operating systems, software, and hardware has been extremely cost effective and simplified network management. Homogeneity also increases the Air Force's capability to garner the situational awareness necessary for effective command and control. However, movement to a centralized architecture with standardized configurations also introduces the risk of a targeted attack being extremely disruptive.

Since conflict in cyberspace is new and dynamic, it is vulnerable to what Nassim Taleb describes as a *Black Swan*, "the extreme, the unknown, and the very improbable." To mitigate against a disaster caused by an extreme event, the Air Force must prepare a range of options and organizations that are less susceptible to total failure; possibly posturing to sometimes lose small to win big.[5] As predicted in "Cyber War is Coming", "waging cyberwar may require major innovations in organizational design, in particular a shift from hierarchies to networks. The traditional reliance on hierarchical designs may have to be adapted to network-oriented models to allow greater flexibility, lateral connectivity, and teamwork across institutional boundaries."[6] Hierarchical command and control approaches that attempt to achieve perfect situational awareness and centralized control will fail in the face of an active thinking enemy.

War is a complex and chaotic activity that cannot be controlled in a precise, predictable way. The unique characteristics of cyberspace must define the problem space and should define the command and control approach. Using the six aspects of agility to determine where in the approach space cyberspace command and control should reside, the hybrid-network proposed is best suited to address the problem space and approach to command and control of Air Force cyberspace. This approach provides the most agility

[5] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York, NY: Random House, 2007), xxvii-xxviii.
[6] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," in *In Athena's Camp: Preparing for Conflicts in the Information Age*, ed. John Arquilla and David Ronfeldt (Washington DC: RAND, 1997), 45.

to cope with the dynamic, near speed of light environment and still provide a mechanism to centralize control when necessary.

Recommendations

To prepare an agile organization that can adapt to the challenges of cyberspace, the Air Force "must concentrate less on determining specific actions to be taken and far more on manipulating the structure within which all actions are determined."[7] Since achieving and maintaining broad cyberspace superiority cannot be assured, the initial conditions must be set to *allow* success to happen. The enabling concept for command and control of cyberspace says that the 624 OC must control the decision cycle to make timely accurate decisions, and execute those decisions faster than the adversary.[8] A reactive approach to network defense does not allow for a rapid process across the AFIN. A more proactive and survivable approach that encompasses network structure, training, and proper rules of engagement are necessary for cyberspace operations to support mission assurance.

Martin Libicki proposes there are two ways that information systems deal with noise in a system, the castle and the agora.[9] A castle is a noise intolerant system that protected against noise by building bigger walls. For example, the Air Force protects the command and control systems as castles by creating isolated networks, disconnected from outside networks. There are benefits to this system, by only having one entry and exit point into the castle, defenders must protect only one place. However, if the intruder breaches the wall, they have full access and can completely disrupt information flow.[10] A danger of the castle approach is it may be self-defeating; if the response to enemy attacks is to further restrict and close off information flows, the defense effectively accomplishes what the attacker intended.[11]

---

[7] Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York, NY: FRANK CASS, 2005), 4.
[8] Air Force Space Command (AFSPC), *Enabling Concept for Command and Control of Cyberspace Forces*, 19 January 2010, 5.
[9] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 62.
[10] Libicki, *Conquest in Cyberspace*, 63.
[11] Libicki, *Conquest in Cyberspace*, 70.

In contrast, the agora is a noise-tolerant environment that "opens up as many paths as necessary to negate the effect of the noise."[12] Multiple paths increase the possibility to get the correct information through the noise of an attack. If attacks take place on multiple channels and only partial information gets through on each channel, then situational awareness can be enhanced by comparing information received on each channel to determine the validity of the information or to consolidate all information received to create a fused picture.[13]

The objective for the Air Force must be to build systems and organizations that can more effectively deal with uncertainty. Command and control systems must be able to cope with noise in the communications channel. If the enemy is attempting to cause noise instead of merely denying service, it may be more disruptive because it can have a permanent effect on decision-making. Commanders could lose confidence in the information provided by the information systems. This challenge is no different than what commanders have had to cope with throughout the history of command; consolidating all the information available, discarding the less believable information, fusing the credible, and using commander's intuition to act.

Creating diversity of information paths, systems, and operational processes is necessary in cyberspace. Creating multiple information paths through redundancy has long been a communication planner's basic way of coping with uncertainty, but diversity of systems has been viewed as a problem. Multiple types of systems are not cost effective, they are more difficult to operate, maintain, and increase personnel training costs. However, focusing on cost alone may be short-sighted, when the object of an attack is a particular fault in specific system, the attack can spread more rapidly in a homogenous system, than one more diverse. Commanders must achieve a balance between efficiency and effectiveness in war, where "efficiency, far from being simply conducive to effectiveness, can act as its opposite."[14]

Twenty-fourth Air Force understands it cannot guarantee uninterrupted access to cyberspace across the domain. While conflicts over the past two decades have created

---

[12] Libicki, *Conquest in Cyberspace*, 62.
[13] Libicki, *Conquest in Cyberspace*, 63.
[14] Martin van Creveld, *Technology and War: From 2000 B.C. to the Present* (New York, NY: The Free Press, 1989), 319.

the impression that the United States can operate unopposed in cyberspace; this will not remain the case. In a major conflict, it is likely well-trained competitors will attack multiple US information systems simultaneously and repeatedly. To prepare, it is imperative operators in all domains create tactics, techniques, and procedures to cope with the loss of information systems and fight through attacks.[15] Exercises that practice this in peacetime will prepare commanders to cope with imperfect and incomplete information during conflict.

Training of cyberspace forces is critical for an agile command and control structure to be successful. Highly trained forces that understand their weapon system, achieve high standards, and are certified to operate in dynamic situations conduct air and space power operations. The Air Force must train and hold accountable the cyber operator to the same standards as air and space. Until recently, communications officer training has consisted of a short course to increase awareness of Air Force communications systems, units, and missions. Little technical expertise was required of officers, the knowledge of how to install, operate, and maintain communications systems has traditionally resided with enlisted technicians.

A concerted effort to recruit officers from degree programs in information systems, computer science, and computer and electrical engineering will provide the technical background to begin training cyberspace operations officers. Cyberspace officers must receive a holistic education in Air Force operations and cyberspace's role in the mission. Once trained, they will be able to innovate through the development of applications and implementation of available technology. Operators should write applications at the local level to solve local problems. Through training, clear rules of engagement, and accountability for what the cyberspace operator implements on the network, innovation can take place at the pace necessary in the information age.

The trend to eliminate cyberspace experts at the wing level could lead to a force unable to respond when cut off from the centralized control and expertise of the global cyberspace command and control center. The centralization of network services is a bet that the United States can always maintain cyberspace superiority. Although many services are still operated at the wing level, communications squadron commanders who

[15] Colonel Victor Diaz (commander, 624 Operations Center), interview by the author, 22 March 2010.

have or currently are serving in the AFCENT AOR complain of poor communication and service received from the network operations and support center in the United States. Issues with timeliness and response during main hours of operation in the theater of operations suffer when the network control center is on a normal duty schedule in the US Eastern Time zone.[16] The ultimate danger however, is "the more centralized the system, the greater the danger that it will be paralyzed if enemy action causes the directing brain to be eliminated or communication with it to be impaired."[17] The development of cyber warfare personnel with the proper level of authority and accountability are necessary to ensure the cyberspace domain is available when required.

Sun Tzu wrote 2,500 years ago, "Know the enemy and know yourself; in a hundred battles you will never be in peril."[18] Situational awareness on the network is just as essential today to facilitate the most optimal function of the hybrid-network approach. Twenty-fourth Air Force is working to achieve situational awareness at the 624 OC; however, they must also share this information with the NCCs. The NCCs can filter information not necessary for daily operations and expand the view when needed. Information sharing with higher-echelons, to subordinate units, and laterally will allow the proper echelon to operate, maintain, and conduct offensive operations when necessary.

Cyberpower must be made available to operational forces; the over-classification of cyber capabilities can limit the possible effects offensive cyberpower can offer the combatant commander. There are certainly tactics and targets the United States must guard closely and should remain centralized at the highest levels. However, many types of attacks are well known in the public domain, but can still be very effective against weak or unprotected systems. Proper rules of engagement will allow CNA units the freedom to act, seize the initiative, and take advantage of fleeting opportunities.

---

[16] Response to a discussion question by author to several commanders in the AFCENT AOR. "Is the NOSC responsive to your requests for support?" January 2010.
[17] Creveld, *Technology and War*, 317.
[18] Sun Tzu, *The Illustrated Art of War*, trans. Samuel B. Griffith (New York, NY: Oxford University Press, 2005), 125.

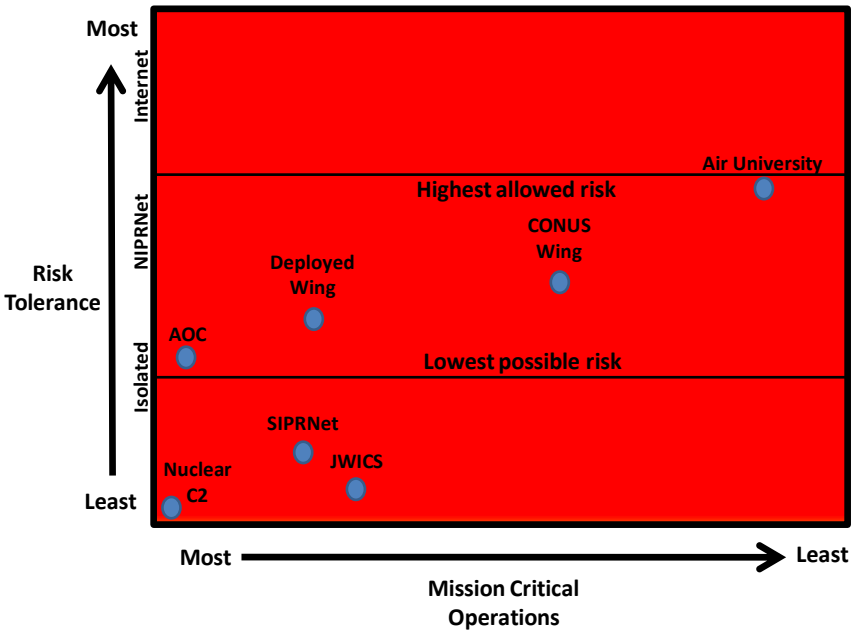

Figure 11: Cyberspace Risk Posture
Source: Author's Own Work

The Air Force can also use clear rules of engagement to determine the amount of risk a wing is allowed to accept. As depicted in Figure 11, the operation and defense of the AFIN can be depicted through the a cyberspace risk posture. If trained, the communications squadron commander can advise the wing commander on an appropriate level of risk for the portion of the AFIN the wing operates. The risk assessment is determined by the mission critical nature of the network to wing operations and the risk tolerance for loss of service or information that traverses the network. A unit may not reside solely in one position in this box, but move according to current operations. For example, a deployed unit may be more risk averse before and during a major operation, but return to a more risk tolerant posture during normal sustainment operations. The Air Force has implemented a robust defense-in-depth approach that assures a risk to one is not a risk to all. For example, the NIPRNet is connected to the open Internet and the AFIN is connected to the Army and Navy networks which apply slightly different security standards and allow different services to traverse their portion of the GIG. These

approaches attempt to allow some local control and the ability to create value at the wing level while still maintaining connectivity to the central cyberspace control element.

War, ultimately a human endeavor, is a social phenomenon and defies man's efforts to create doctrine and theory that can prescribe the best way to execute. The decisions made today about the best command and control approach for cyberspace will determine how the Air Force is postured to survive, respond, and assure operations in the air and space domains in future conflicts. Cyber warfare personnel with the proper training, authority, and accountability are vital to ensure the cyberspace domain is available when required. Innovative leaders must take steps now to ensure the organization and command and control approach will remain agile enough to respond to the demands of the other domains while protecting cyberspace capabilities. An agile command and control approach will better transition from low-level conflicts to a high-level conflict against a near peer adversary. Cyber warfare at the speed of light will demand this agility.

Bibliography

505th Command and Control Wing. "C/JFACC Processes." *USAF Senior Mentor Training.* Hurlburt Field, FL, September 2007.

Adee, Sally. "The Hunt for the Kill Switch." *ieee spectrum.* May 2, 2008. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch (accessed 5 February 2010).

Air Force Doctrine Document (AFDD) 1. *Air Force Basic Doctrine.* November 17, 2003.

Air Force Doctrine Document (AFDD) 2. *Operations and Organizations.* 3 April 2007.

Air Force Doctrine Document (AFDD) 2-1.9. *Targeting.* 3 June 2006.

Air Force Doctrine Document (AFDD) 2-2. *Space Operations.* 27 November 2006.

Air Force Doctrine Document (AFDD) 2-8. *Command and Control.* 1 June 2007.

Air Force Doctrine Document (AFDD) 3-12 (Draft). *Cyberspace Operations.* XX March 2010.

Air Force Space Command. *Enabling Concept for Command and Control of Cyberspace.* 19 January 2010.

—. *The United States Blueprint for Cyberspace.* 2 November 2009.

Alberts, David S., and Richard E. Hayes. *Power to the Edge.* Washington DC: DoD Command and Control Research Program, 2003.

—. *Understanding Command and Control.* Washington, DC: DoD Command and Control Research Program, 2006.

Alberts, David S., John J. Garstka, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority.* 2nd Edition. Washington DC: DoD C4ISR Cooperative Research Program, 1999.

Allard, C. Kenneth. *Command, Control, and The Common Defense.* New Haven, CT: Yale University Press, 1990.

Arquilla, John, and David Ronfeldt. "Cyberwar is Coming!" In *In Athena's Camp: Preparing for Conflicts in the Information Age*, edited by John Arquilla and David Ronfeldt, 23-60. Washington DC: RAND, 1997.

Brate, Adam. *Technomanifestos.* New York, NY: TEXERE LLC, 2002.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York, NY: Oxford University Press, 2009.

Chandler, David G. *The Campaigns of Napoleon.* New York, NY: Scribner, 1966.

Clausewitz, Carl Von. *On War.* Translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.

Corbett, Julian Stafford. *Some Principles of Maritime Strategy.* Annapolis, MD: Naval Institute Press, 1988.

Craig, Campbell. *Destroying the Village: Eisenhower and Thermonuclear War.* New York, NY: Columbia University Press, 1998.

Creveld, Martin van. *Command In War.* Cambridge, MA: Harvard University Press, 1985.

—. *Technology and War: From 2000 B.C. to the Present.* New York, NY: The Free Press, 1989.

Department of Defense (DOD) 8000.1. *Management of the Department of Defense Information Enterprise.* 10 February 2009.

Department of Defense. *The National Military Strategy for Cyberspace Operations.* Washington DC: Department of Defense, December 2006.
Department of the Air Force. "Fiscal Year 2010 Air Force Posture Statement." Presenation to the Senate Armed Services Commitee, United States Senate, 21 May 2009.
Dolman, Everett Carl. *Pure Strategy: Power and Principle in the Space and Information Age.* New York, NY: Frank Cass, 2005.
Drew, Christopher. "Drones Are Weapons of Choice in Fighting Qaeda." *The New York Times.* Mar 16, 2009. http://www.nytimes.com/2009/03/17/business/17uav.html (accessed 9 February 2010).
Easton, Ian. "The Great Game in Space: China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy." *The Project 2049 Institute.* http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf (accessed 25 April 2010).
Fuller, J.F.C. *The Foundations of The Science of War.* London: Hutchinson & Co., LTD., 1926.
Gates, Robert M., Secretary of Defense. "To secretaries of the Militrary Departments, Chairman of the Joint Chiefs of Staff, Under Secretaries of Defense, Commanders of the Combatant Commanders, Assistant Secretaries of Defense, Memorandum ." June 23, 2009.
Gibson, William. "Burning Chrome." In *Burning Chrome*, 179. New York, NY: HarperCollins Publishers Inc, 1984.
—. *Neuromancer.* New York, NY: The Penguin Group, 1984.
Hammond, Grant T. *The Mind of War: John Boyd and American Security.* Washington, DC: Smithsonian Books, 2001.
Hinote, Lt Col Clint. "Centralized Control and Decentralized Execution: A Catchphrase in Crisis?" *Air Force Research Institute Papers* . Maxwell AFB, AL: Air University, Air Force Research Institute, March 2009.
Hobbins, Lt Gen William Thomas. "Airmen on the Battlefield: Warfighting Integration in Support of Special." *Air and Space Power Journal* XIX, no. 1 (Spring 2005): 67-79.
Horne, Alistair. *The Price of Glory, Verdun 1916.* London: The Penguin Group, 1993.
Howard, Michael. "Men against Fire: The Doctrine of the Offensive in 1914." In *Makers of Modern Strategy*, edited by Peter Paret, 510-526. Princeton, NJ: Princeton University Press, 1986.
Hughes, Thomas A. *OVER LORD.* New York, NY: The Free Press, 1995.
Hugill, Peter J. *Global Communications Since 1844: Geopolitics and Technology.* Baltimore: John Hopkins University Press, 1999.
Internet Systems Consortium. *The ISC Domain Survey.* https://www.isc.org/solutions/survey (accessed 24 May 2010).
Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms.* 12 April 2001 (As Amended Through 31 October 2009).
Joint Publication 3-30. *Command and Control for Joint Air Operations.* 12 January 2010.
Joint Publication 3-60. *Joint Targeting.* 13 April 2007.
Keegan, John. *The Face of Battle.* New York, NY: Penquin Books, 1976.
Kennett, Lee. *The First Air War: 1914-1918.* New York, NY: Free Press, 1991.

Kometer, Michael W. *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower.* Maxwell Air Force Base, AL: Air University Press, 2007.
Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 24-42. Washington, DC: National Defense University Press, 2009.
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge, England: Cambridge University Press, 2006.
Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future.* London: Frank Cass, 2004.
McDougall, Walter A. *...The Heavens and The Earth: A Political History of the Space Age.* Baltimore, MD: The Johns Hopkins University Press, 1985.
Moltke, Helmuth von. *Moltke on the Art of War.* Edited by Daniel J. Hughes. New York, NY: Ballantine Books, 1993.
Morrow, John H. Jr. *The Great War in the Air, Military Aviation from 1909 to 1921.* Tuscaloosa: The University of Alabama Press, 1993.
Mortensen, Daniel R. "The Air Service in the Great War." In *Winged Shield, Winged Sword, Volume I,* edited by Bernard C. Nalty. Washington DC: United States Air Force, 1997.
Murray, Williamson. "Strategic bombing: The British, American, and German experiences." In *Military Innovation in the Interwar Period,* edited by Williamson Murray and Allan R. Millett, 96-143. New York, NY: Cambridge University Press, 1996.
Nalty, Bernard C. "The Defeat of Italy and Germany." In *Winged Shield, Winged Sword, Volume I,* edited by Bernard C. Nalty, 269-326. Washington DC: United States Air Force, 1997.
Nalty, Bernard C., ed. *Winged Shield, Winged Sword, Volume I.* Washington, DC: United States Air Force, 1997.
Obama, Barack, The President. "REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S INFRASTRUCTURE." *The White House.* May 29, 2009. http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed 11 February 2010).
Office of the Command Historian. "A Concise History of the U.S. Army Signal Corps." Fort Gordon: US Army Signal Center, January 25, 1994.
Overy, Richard J. *The Air War, 1939-1945.* Dulles: Potomac Books, Inc., 2005.
—. *The Battle of Britian.* New York: W.W. Norton & Company, Inc., 2002.
Parker, Geoffrey, ed. *The Cambridge History of Warfare.* New York: Cambridge University Press, 2005.
Pearson, David E. *The World wide Military Command and Control System : Evolution and Effectiveness.* Maxwell AFB, AL: Air University Press, 2000.
Putney, Diane T. *Airpower Advantage: Planning the Gulf War Air Campaign 1989-1991.* Washington DC: United States Air Force, 2004.
Rattray, Gregory J. "An Environmental Approach to Understanding Cyberpower." In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 253-274. Washington, D.C.: National Defense University Press, 2009.

Rife, Maj Shawn P. "Kasserine Pass and the Proper Application of Airpower." *Joint Force Quarterly*, Autumn/Winter 1998-99: 71-77.
Rip, Michael Russel, and David P. Lusch. "The Precision Revolution: The Navstar Global Positioning System in the Second Gulf War." *Intelligence and National Security* 9, no. 2 (April 1994): 171.
Roman, Gregory A. *The Command and Control Dilemma: When Technology and Organizational Orientation Collide.* Air Force 2025 Study, Maxwell AFB, AL: Center for Strategy and Technology, 1996.
Rotenberg, Gunther E. "Moltke, Schlieffen, and the Doctrine of Strategic Envelopment." In *Makers of Modern Strategy*, edited by Peter Paret, 299. Princeton, NJ: Princeton University Press, 1986.
Schwartz, Gen Norton A. "Chief of Staff, US Air Force, to ALMAJCOM-FOA-DRU/CC, memorandum." May 15, 2009.
Secretary and Chief of Staff of the Air Force to All Airmen. memorandum, August 20, 2009.
Secretary of Defense. *National Military Strategy for Cyberspace Operations.* Washington D.C.: Department of Defense, 2006.
Sheehan, Michael. *The International Politics of Space: No Final Frontier.* New York, NY: Routledge, 2007.
Spires, David N. *Beyond Horizons: A Half Century of Air Force Space Leadership.* Maxwell AFB: Air University Press, 1998.
Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable.* New York, NY: Random House, 2007.
The White House. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." 2009.
Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Anna-Maria Talihärm Mari Kert, and Liis Vihul. *Cyber Attacks Against Georgia: Legal Lessons Identified.* Analysis, Tallin, Estonia: Cyber Cooperative Centre of Excellence, 2008.
Tzu, Sun. *The Illustrated Art of War.* Translated by Samuel B. Griffith. New York, NY: Oxford University Press, 2005.
US Army Program Manager. *Force XXI Battle Command Brigade and Below.* http://peoc3t.monmouth.army.mil/fbcb2/fbcb2.html (accessed 5 May 2010).
War Department Field Manual 100-20. *Field Service Regulations, Command and Employment of Air Power.* 21 July 1943.
Westermann, Edward B. *Flak.* Lawrence, KS: University Press of Kansas, 2001.